HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme
Praktikum 3

Bundeskriminalamt

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

13.04.2023

Agenda

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

Praktikum 3

1. Vorbereitung/Voraussetzungen

1. Vorbereitung/Voraussetzungen

Virtualisierungssoftware:

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

DVD Abbilddatei (*ISO*):

- **PR2.iso**

Hostsystem:

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

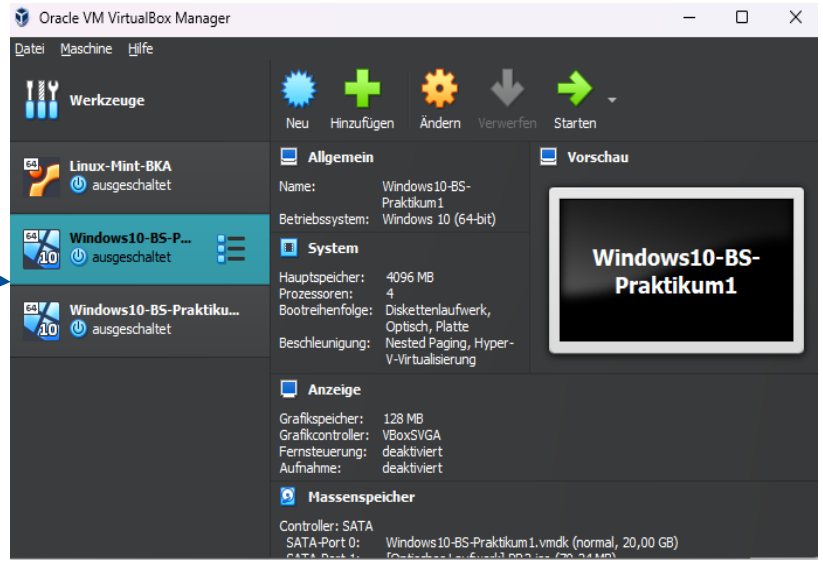


Abb. 1

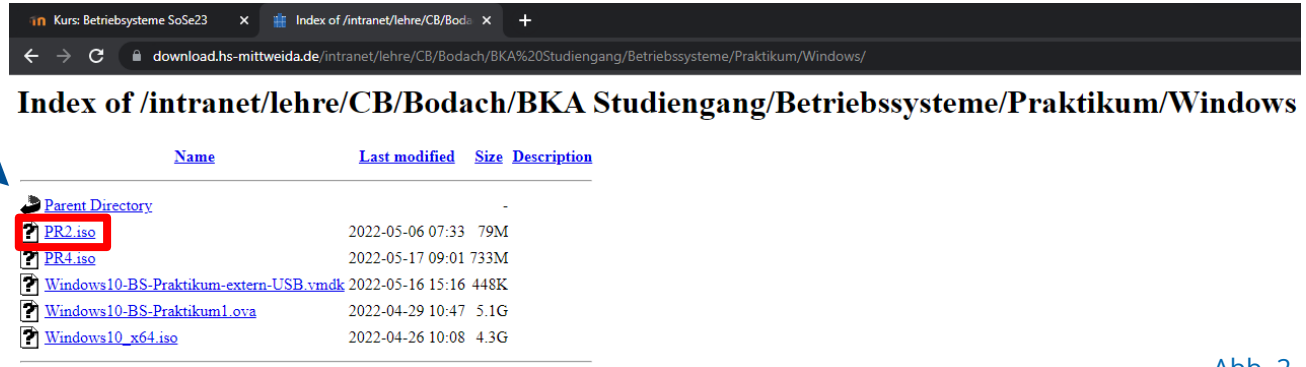


Abb. 2

1. Vorbereitung/Voraussetzungen

Allgemeine Hinweise:

Kopieren Sie bitte die ISO Datei **PR2.iso (75MB)** auf ihre lokale Festplatte in ein separates Verzeichnis auf das Sie Zugriff haben, bestenfalls in das VM Verzeichnis von Praktikum1.

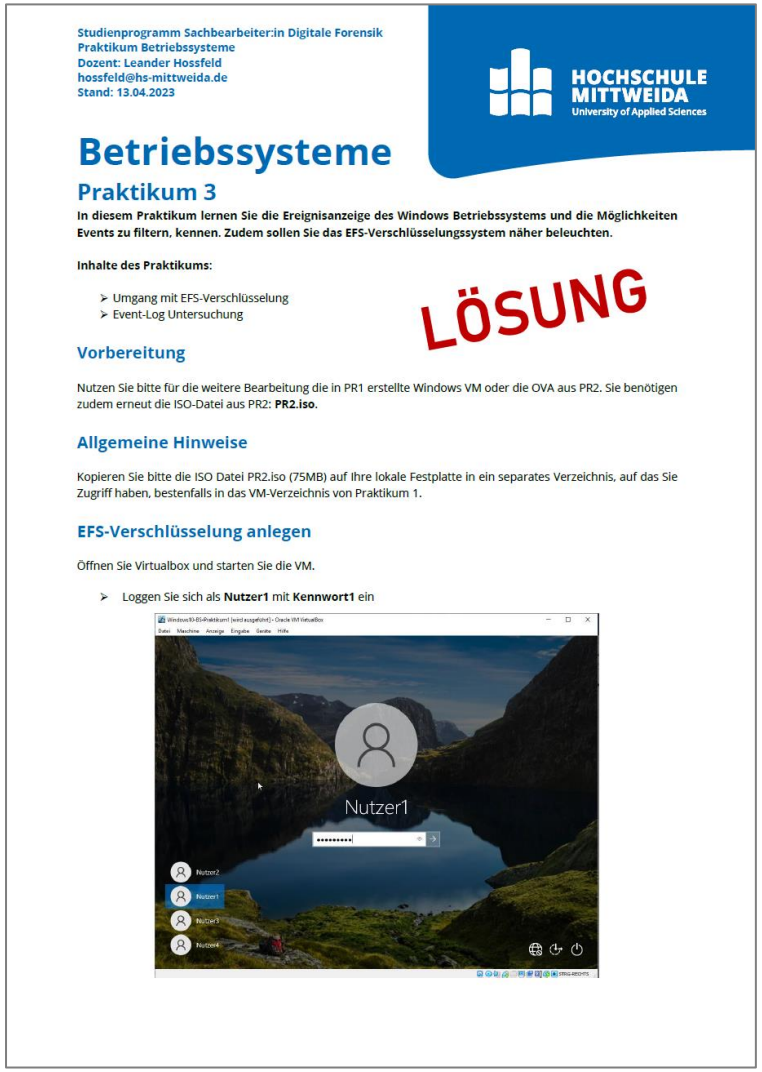
Abb. 3

Praktikum 3

2. Aufgabenbesprechung

2. Aufgabenbesprechung

- Umgang mit EFS-Verschlüsselung
- Event-Log Untersuchung



Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 13.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum 3

In diesem Praktikum lernen Sie die Ereignisanzeige des Windows Betriebssystems und die Möglichkeiten Events zu filtern, kennen. Zudem sollen Sie das EFS-Verschlüsselungssystem näher beleuchten.

Inhalte des Praktikums:

- Umgang mit EFS-Verschlüsselung
- Event-Log Untersuchung

LÖSUNG

Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2. Sie benötigen zudem erneut die ISO-Datei aus PR2: **PR2.iso**.

Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei PR2.iso (75MB) auf Ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum 1.

EFS-Verschlüsselung anlegen

Öffnen Sie Virtualbox und starten Sie die VM.

- Loggen Sie sich als **Nutzer1** mit **Kennwort1** ein

Abb. 4

Praktikum 3

3. Durchführung/Ziel

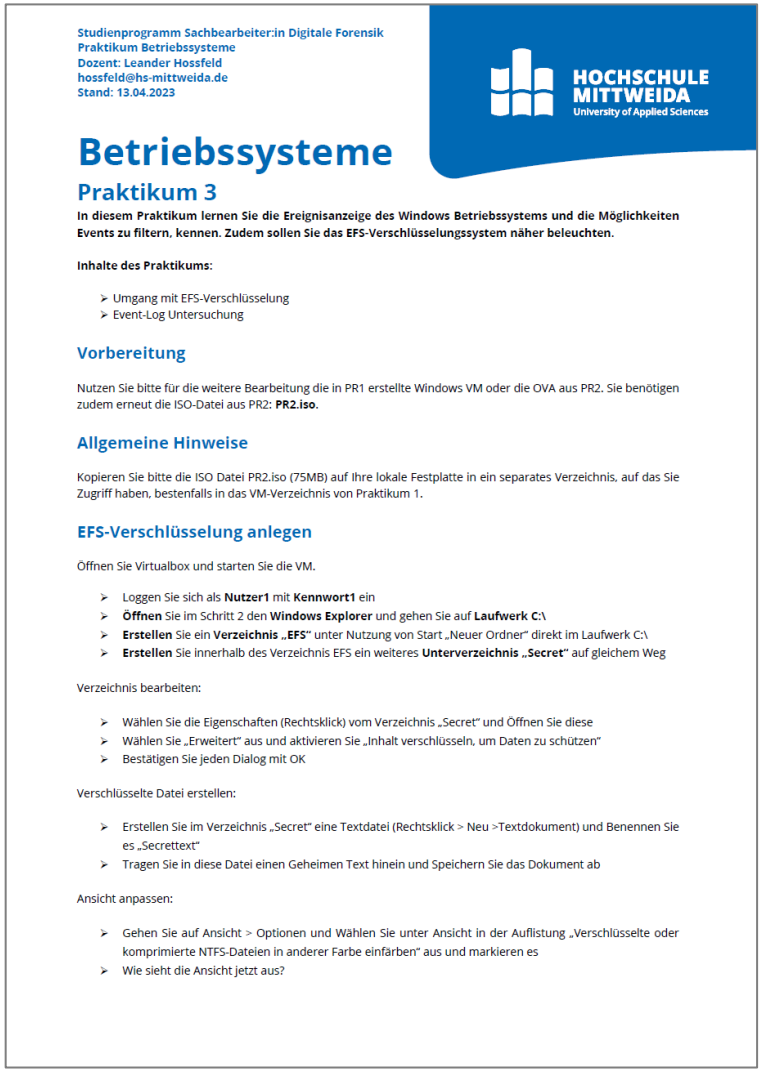
3. Durchführung/Ziel

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:

- Kennenlernen der Ereignisanzeige des Windows Betriebssystems und die Möglichkeiten Events zu filtern.
- EFS-Verschlüsselungssystem näher beleuchten
- Verständnis und Vertiefung der theoretischen Inhalte



Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 13.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum 3

In diesem Praktikum lernen Sie die Ereignisanzeige des Windows Betriebssystems und die Möglichkeiten Events zu filtern, kennen. Zudem sollen Sie das EFS-Verschlüsselungssystem näher beleuchten.

Inhalte des Praktikums:

- Umgang mit EFS-Verschlüsselung
- Event-Log Untersuchung

Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2. Sie benötigen zudem erneut die ISO-Datei aus PR2: **PR2.iso**.

Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei PR2.iso (75MB) auf Ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum 1.

EFS-Verschlüsselung anlegen

Öffnen Sie Virtualbox und starten Sie die VM.

- Loggen Sie sich als **Nutzer1** mit **Kennwort1** ein
- **Öffnen** Sie im Schritt 2 den **Windows Explorer** und gehen Sie auf **Laufwerk C:**
- **Erstellen** Sie ein **Verzeichnis „EFS“** unter Nutzung von Start „Neuer Ordner“ direkt im Laufwerk C:\
- **Erstellen** Sie innerhalb des Verzeichnis EFS ein weiteres **Unterverzeichnis „Secret“** auf gleichem Weg

Verzeichnis bearbeiten:

- Wählen Sie die Eigenschaften (Rechtsklick) vom Verzeichnis „Secret“ und Öffnen Sie diese
- Wählen Sie „Erweitert“ aus und aktivieren Sie „Inhalt verschlüsseln, um Daten zu schützen“
- Bestätigen Sie jeden Dialog mit OK

Verschlüsselte Datei erstellen:

- Erstellen Sie im Verzeichnis „Secret“ eine Textdatei (Rechtsklick > Neu >Textdokument) und Benennen Sie es „Secrettext“
- Tragen Sie in diese Datei einen Geheimen Text hinein und Speichern Sie das Dokument ab

Ansicht anpassen:

- Gehen Sie auf Ansicht > Optionen und Wählen Sie unter Ansicht in der Auflistung „Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe einfärben“ aus und markieren es
- Wie sieht die Ansicht jetzt aus?

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