



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Grundlagen Digitale Forensik Linux

Laura Pistorius



Bundeskriminalamt

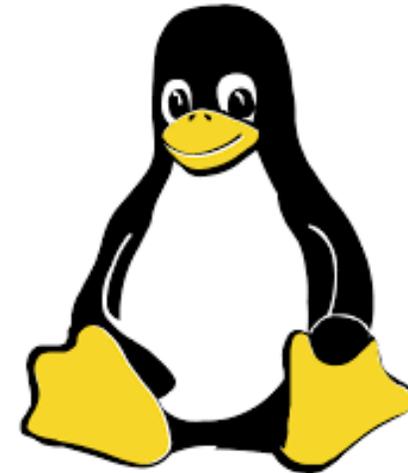
[hs-mittweida.de](https://www.hs-mittweida.de)

Betriebssysteme

- Die Hardware eines Computers allein reicht nicht! Das Betriebssystem ist das Bindeglied zwischen der Hardware und dem Anwender bzw. dessen Anwendungsprogramm(en).
- Gleichzeitig bietet es dem Benutzer zahlreiche Dienste (Programme, Kommandos) an, die zusammen mit den Eigenschaften des Computers die „Grundlage der möglichen Betriebsarten dieses Systems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen“ (DIN 44300).

Linux

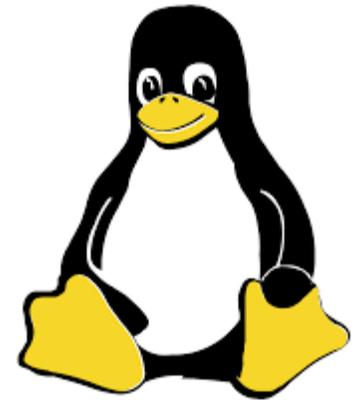
- Betriebssystem
- Verschiedenste Linux-Distributionen
- Open Source Software
- Offenheit und Vielfältigkeit als größter Vorteil
- Den tiefen Einblick übernimmt Professor Bodach ;-)



Linux

Eigenschaften von Linux/UNIX

- (präemptives) Multitasking-System (quasi gleichzeitige Abarbeitung mehrerer Programme/Prozesse/Tasks)
- Multiuser-System
- Mehrere Shells wählbar (in Linux oft bash)
- Mehr als 100 Distributionen, darunter Mint, Debian, Ubuntu, Fedora, Kali, ...



Kali – Das Linux für Digitalforensiker

- open-source und debianbasierte Linux Distribution
- Enthält über 600 nützliche Programme für digitale Forensik und Pentesting
 - Maltego
 - Metasploit
 - Nmap
 - Wireshark
 - John the Ripper
 - ...



Virtuelle Maschinen

- Virtuelle Maschinen sind virtuelle Computer, die dieselben Funktionen wie physische Rechner bieten. Genau wie diese führen virtuelle Maschinen Anwendungen und ein Betriebssystem aus. Bei virtuellen Maschinen handelt es sich jedoch um Computerdateien, die auf einem physischen Computer ausgeführt werden. In anderen Worten: Virtuelle Maschinen agieren als separate Computersysteme. (Quelle: vmware.com)
- Eine virtuelle Maschine (Virtual Machine), auch Gast genannt, wird innerhalb einer als „Host“ bezeichneten Computing-Umgebung ausgeführt. Auf einem Host lassen sich mehrere virtuelle Maschinen gleichzeitig erstellen. Zu den wesentlichen Bestandteilen einer virtuellen Maschine gehören Protokoll-, NVRAM-Einstellungs-, virtuelle Datenträger- und Konfigurationsdateien. (Quelle: vmware.com)

Virtuelle Maschinen – Installation



The screenshot shows the VirtualBox website's download page. On the left is a sidebar with navigation links: About, Screenshots, Downloads, Documentation (with sub-links for End-user docs and Technical docs), Contribute, and Community. The main content area features the VirtualBox logo, a search bar, and links for Login and Preferences. The main heading is 'Download VirtualBox', followed by a paragraph stating that links to binaries and source code are provided. Below this are sections for 'VirtualBox binaries' and 'VirtualBox 6.1.34 platform packages', each with explanatory text and a list of links to various operating system hosts.

VirtualBox

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

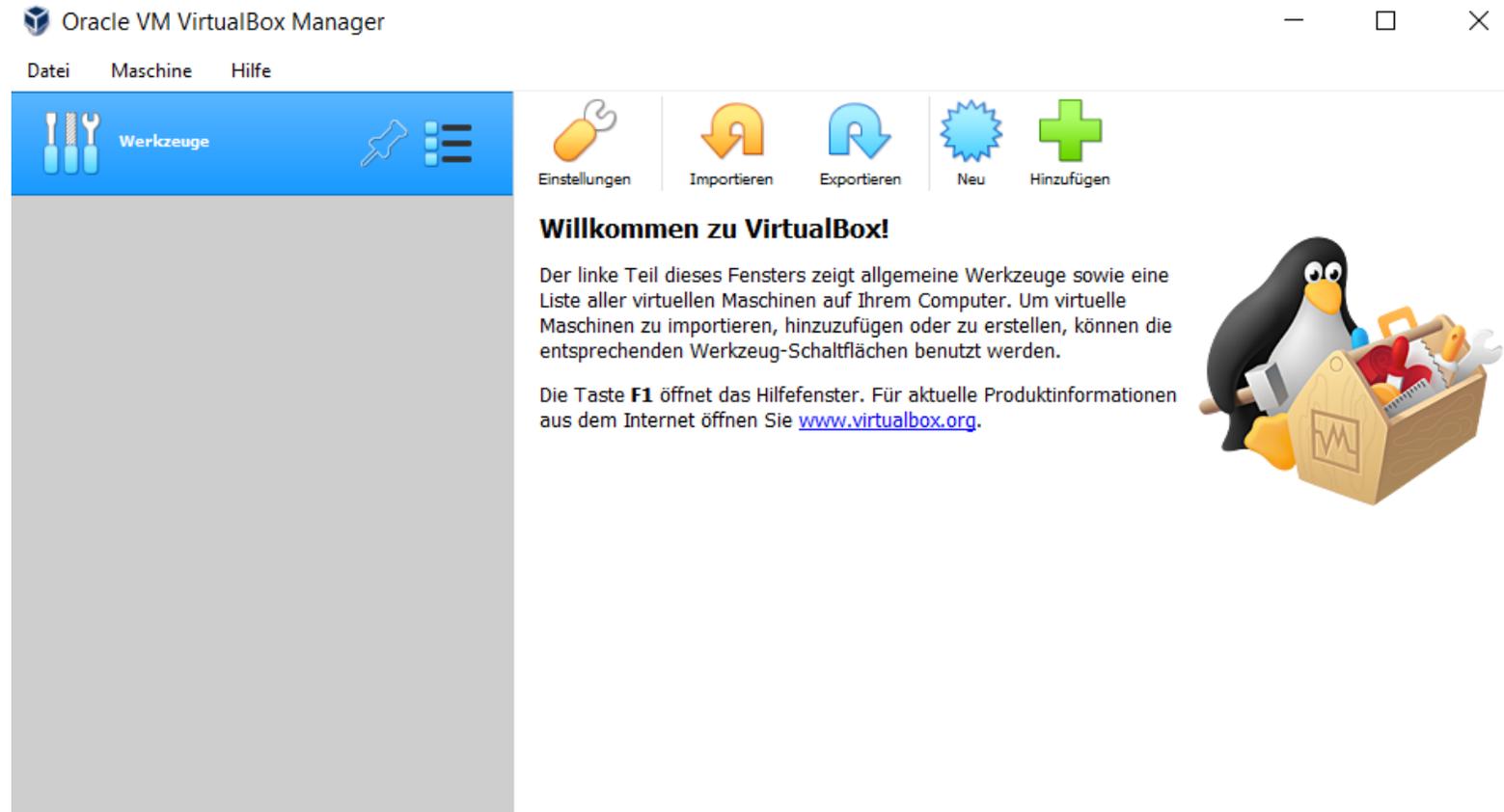
If you're looking for the latest VirtualBox 6.0 packages, see [VirtualBox 6.0 builds](#). Please also use version 6.0 if you need to run VMs with software virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.

If you're looking for the latest VirtualBox 5.2 packages, see [VirtualBox 5.2 builds](#). Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

VirtualBox 6.1.34 platform packages

- [Windows hosts](#)
- [OS X hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

Virtuelle Maschinen – Installation

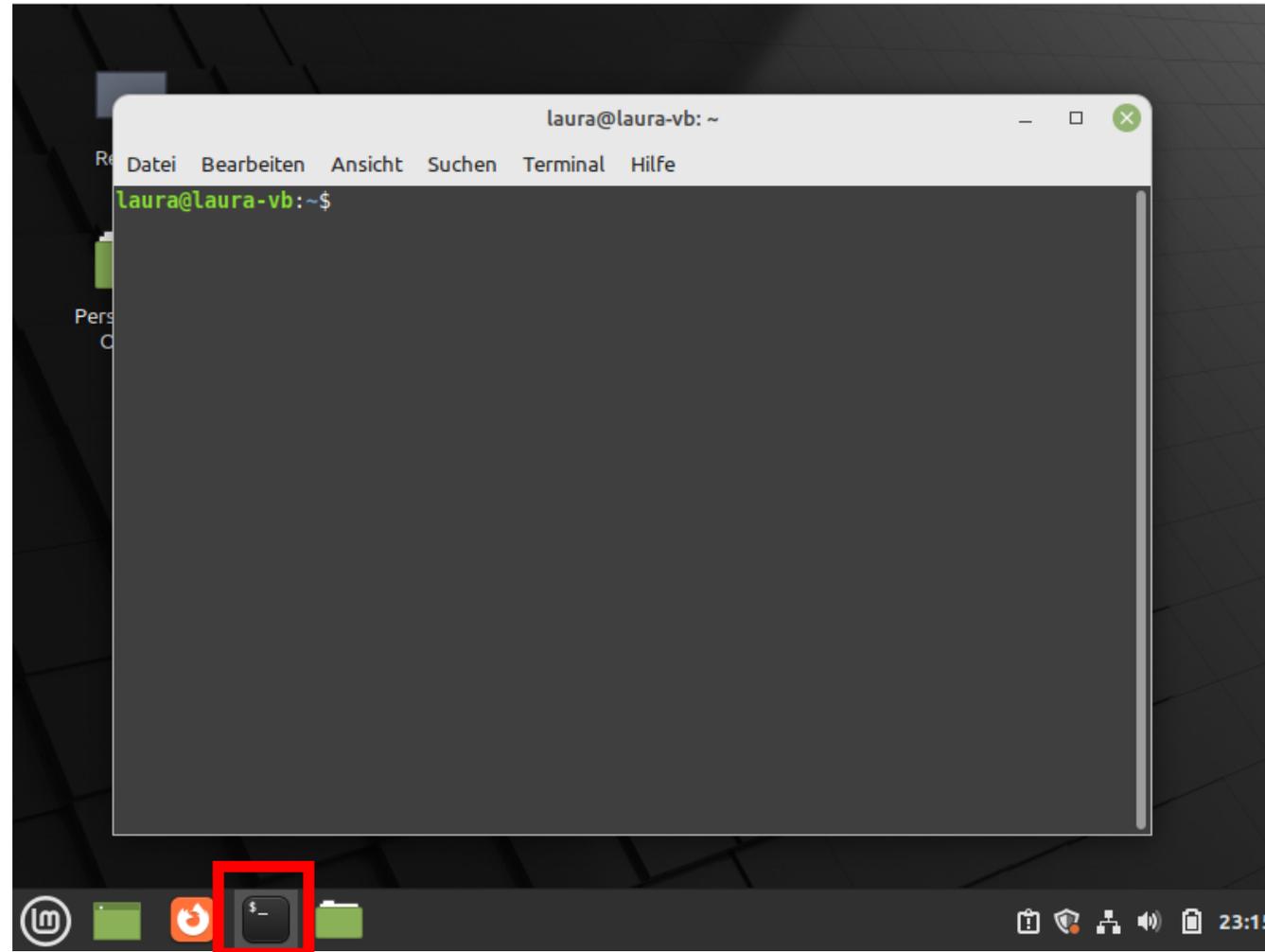


Installationsanleitung finden Sie im Moodlekurs

Linux – Herzlich Willkommen



Linux – Terminal



Vielen Dank



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

B. Sc. Laura Pistorius
Fraunhofer Lernlabor für Cybersicherheit

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

pistori1@hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-107
Musterstraße 123 | 09648 Mittweida

[hs-mittweida.de](https://www.hs-mittweida.de)