HOCHSCHULE MITTWEIDA
University of Applied Sciences

Grundlagen Digitale Forensik
Linux

Laura Pistorius

Bundeskriminalamt

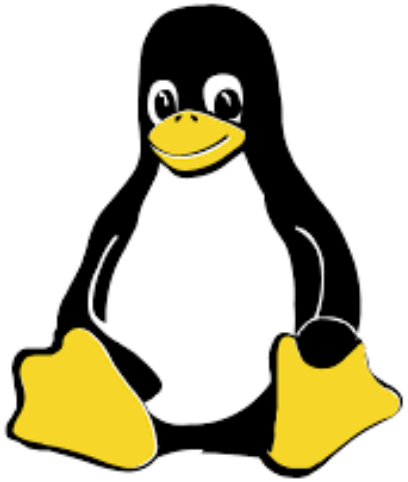
hs-mittweida.de

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

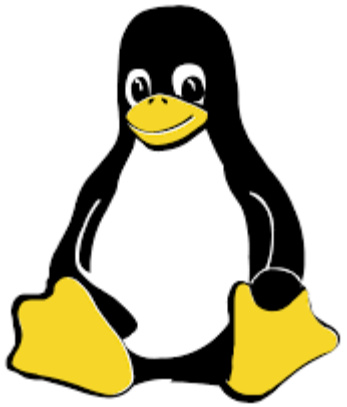
- Betriebssystem
- Verschiedenste Linux-Distributionen
- Open Source Software
- Offenheit und Vielfältigkeit als größter Vorteil
- Den tiefen Einblick übernimmt Professor Bodach ;-)



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

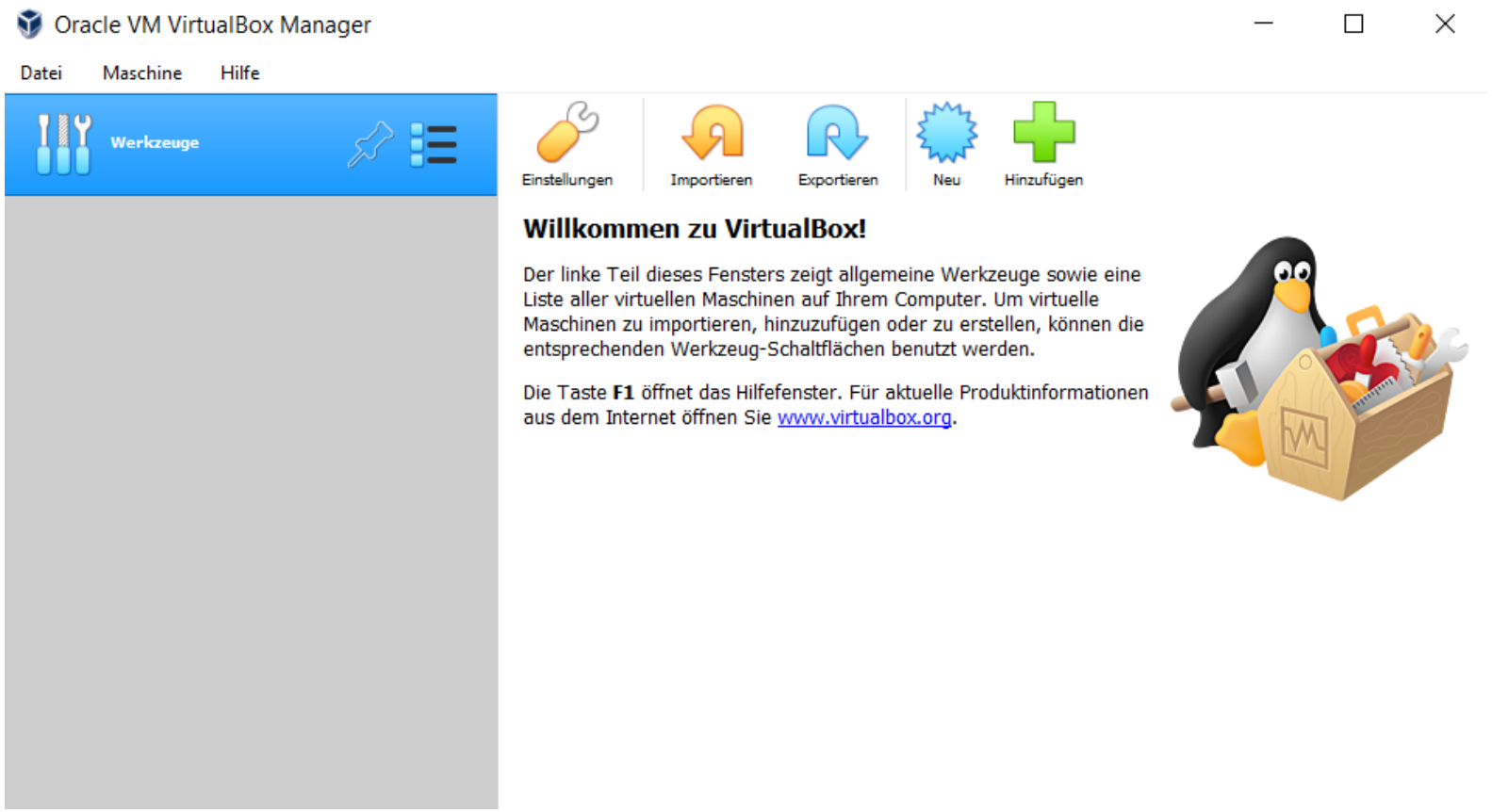
- open-source und debianbasierte Linux Distribution
- Enthält über 600 nützliche Programme für digitale Forensik und Pentesting
  - Maltego
  - Metasploit
  - Nmap
  - Wireshark
  - John the Ripper
  - …

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

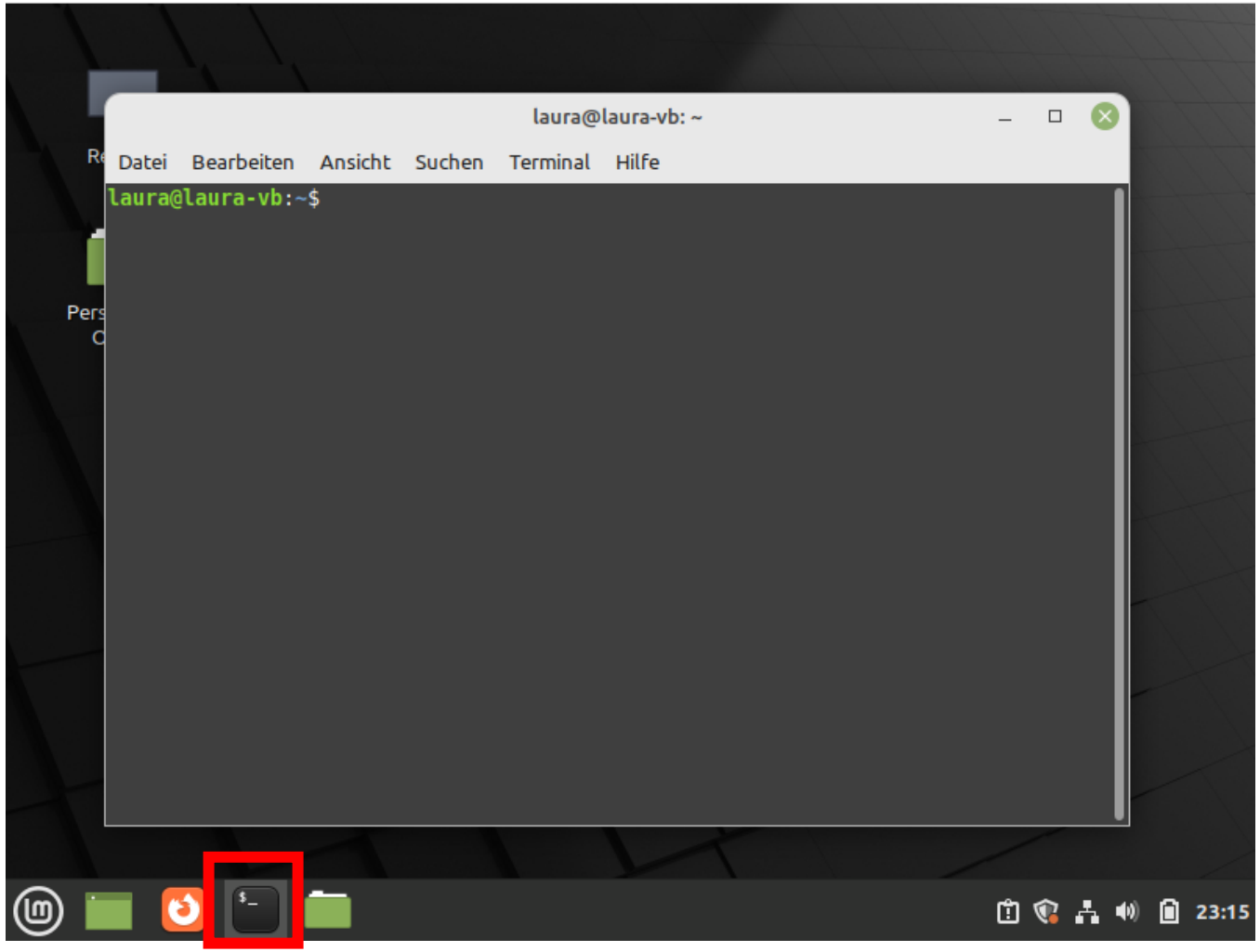
Virtuelle Maschinen – Installation



Installationsanleitung finden Sie im Moodlekurs

Linux – Herzlich Willkommen

Linux – Terminal



Vielen Dank

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

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de