HOCHSCHULE MITTWEIDA
University of Applied Sciences

Bundeskriminalamt

Betriebssysteme
Linux Live Anwendungen

Autor: Wetterau, B.Sc.; Hoßfeld, B.Sc.; Prof. Bodach

Stand: 04.07.2023

Agenda

1. Linux als Live-Distribution
2. Forensische Linux-Distributionen
3. Weitere Live-Distributionen
4. Live-Sicherung am Beispiel von Sumuri PALADIN EDGE

(C) 04.07.2023 Hochschule Mittweida

Linux als Live-Distribution

Warum (Forensic) Live Linux?

Mehrere mögliche Gründe:

- Gewöhnung der sichernden/auswertenden Person
- Tools teils nicht für Windows verfügbar
- Ausbau von Festplatten nicht möglich → fest verlötet
- Risiko der Beschädigung bei Demontage
- Sicherung von Hardware RAID (zusammenhängend)
- Anonymisierung
- Teils keine Persistierungv von Änderungen
- Live-Anwendung hat nur bedingten Einfluss auf Hostrechner

(C) 04.07.2023 Hochschule Mittweida

Voraussetzungen

- Image einer Linux Live Distribution
- Medium mit startfähiger Kopie der Distribution
  - Mit entsprechender Größe
  - Tool zur Erstellung eines Live-Mediums
- Für Live-Boot konfigurierte Boot-Konfiguration
  - Unterstützung durch BIOS/UEFI muss gegeben sein
- Anschlüsse:
  - Für das Live-Medium
  - Für entsprechende Sicherungsplatten
- Ggf. angepasster Kernel für Hardware

(C) 04.07.2023 Hochschule Mittweida

Ziele (Forensic) Live Linux

Möglichkeiten:

- Virensuche & -bekämpfung auf Hostsystem
- Analyse des Systems ohne dieses zwingend zu sichern
- Verhinderung von Schäden durch Demontage von PC-Komponenten

Datensicherung und –analyse unter möglichst forensisch sauberen Vorgehen, ohne das zugrundeliegende System zu verändern.

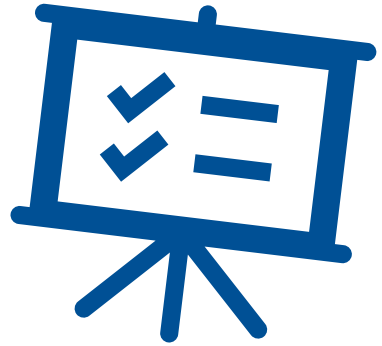
(C) 04.07.2023 Hochschule Mittweida

Forensische Linux-Distributionen

Welches ist das richtige?

Auswahlkriterien

- **Beabsichtigter Zweck der Distribution**
  - Netzwerkforensik
  - Datensicherung
  - Pentesting
- **Verfügbare Tools**
  - Tools sind oftmals je nach Ziel der Distribution verfügbar
  - Sind für die meisten Distributionen verfügbar und oftmals gleichwertig
- **Architektur des zugrundeliegenden Systems**
  - x86
  - x64
  - Arm64
  - etc.



(C) 04.07.2023 Hochschule Mittweida

Kurzübersicht forensischer Distros

- DEFT Linux (www.deftlinux.net)
- CAINE Linux (www.caine-live.net)
- Kali Linux (www.kali.org)
- Sumuri PALADIN (https://sumuri.com/software/paladin/)
- Parrot OS (https://www.parrotsec.org/)

(C) 04.07.2023 Hochschule Mittweida

DEFT Linux

- Fokus auf:
  - Computer Forensik
  - Incident Response
- Herkunft: Italien
- Grundlage: Debian, Lubuntu

(C) 04.07.2023 Hochschule Mittweida

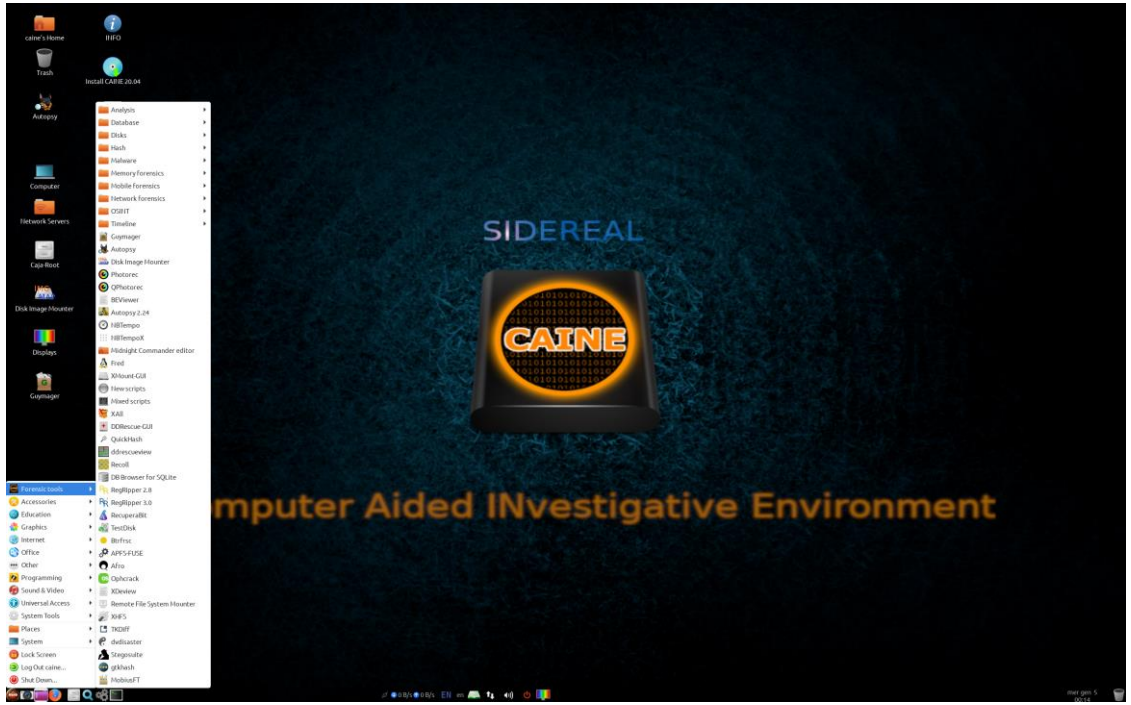
DEFT Linux

- Sehr vollwertige Distribution für forensische Ansprüche
- Viele Tools für Forensiker in einem Paket
- Startfähig von DVD als Live-System
- Nimmt nachweislich so keine Veränderungen am Grundsystem
- Nicht mehr aktuell
  - distrowatch.org: eingestellt

(C) 04.07.2023 Hochschule Mittweida

CAINE Linux

- CAINE = Computer Aided Investigative Environment
- Fokus:
  - Digitale Forensik
  - Interoperable Umgebung verschiedener Module
- Herkunft: Italien
- Grundlage: Debian, Ubuntu



(C) 04.07.2023 Hochschule Mittweida

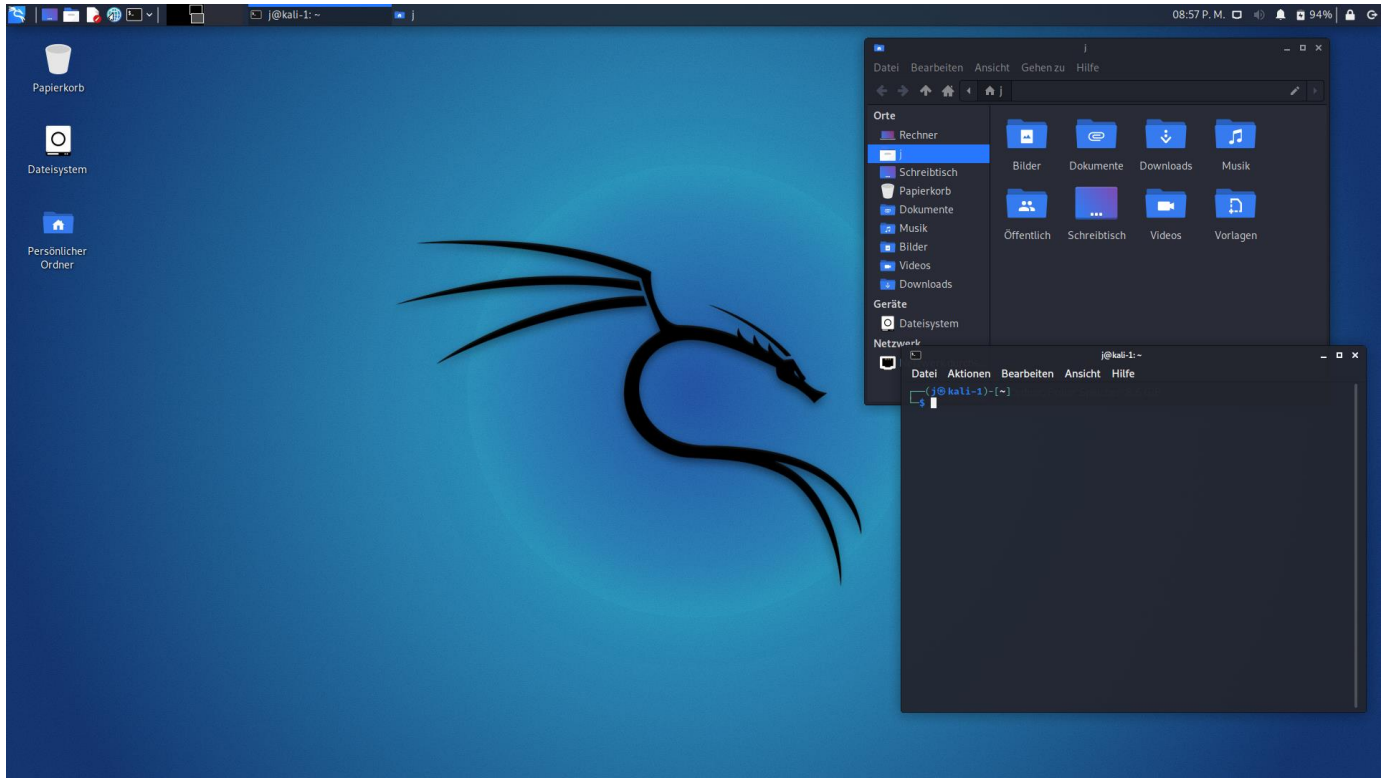
CAINE Linux

- Umfangreiche Tools ähnlich wie DEFT
- Startfähig von UEFI, UEFI Secure Boot, Legacy BIOS
- Alles in einer nutzerfreundlichen GUI zusammengefasst
- Aktiv
  - distrowatch.org
  - Latest Release: CAINE 13.0 WARP (16.03.2023)

(C) 04.07.2023 Hochschule Mittweida

Kali Linux

- Eine der bekanntesten Distributionen im Security Bereich
- Fokus:
  - Pentesting
  - Network Security
- Herkunft: Gibraltar
- Grundlage: Debian



(C) 04.07.2023 Hochschule Mittweida

Kali Linux

- **Trotz verlagertem Schwerpunkt beinhaltet Kali Forensik Tools**
  - Weniger umfangreich
  - Aber erweiterbar
  - Volle Version: Everything (11GB) → https://www.kali.org/get-kali/#kali-live

- **Spezieller forensic Mode als Startoption**
  - Neutral gegenüber der vorhandenen Hardware
  - Keine Persistierungen auf dem Bootmedium

→ Alle Tools zur Datensicherung vorhanden

→ + Tools zum Pentesting oder Untersuchung zu Microsoft AD z.B.

(C) 04.07.2023 Hochschule Mittweida

Sumuri PALADIN

- Sehr moderne Distribution für den forensischen Einsatz
- Fokus:
  - Intuitive Bedienung
  - Vereinfachte Forensik-Anwendungen
- Herkunft: USA
- Grundlage: Ubuntu

(C) 04.07.2023 Hochschule Mittweida

Sumuri PALADIN

- Integrierte Toolbox mit verschiedenen Anwendungen
  - Datensicherung über einfache GUI
  - Verschiedene Formate, per Netzwerk etc.
  - Eingabe forensischer Informationen etc.
  - Data Wiper

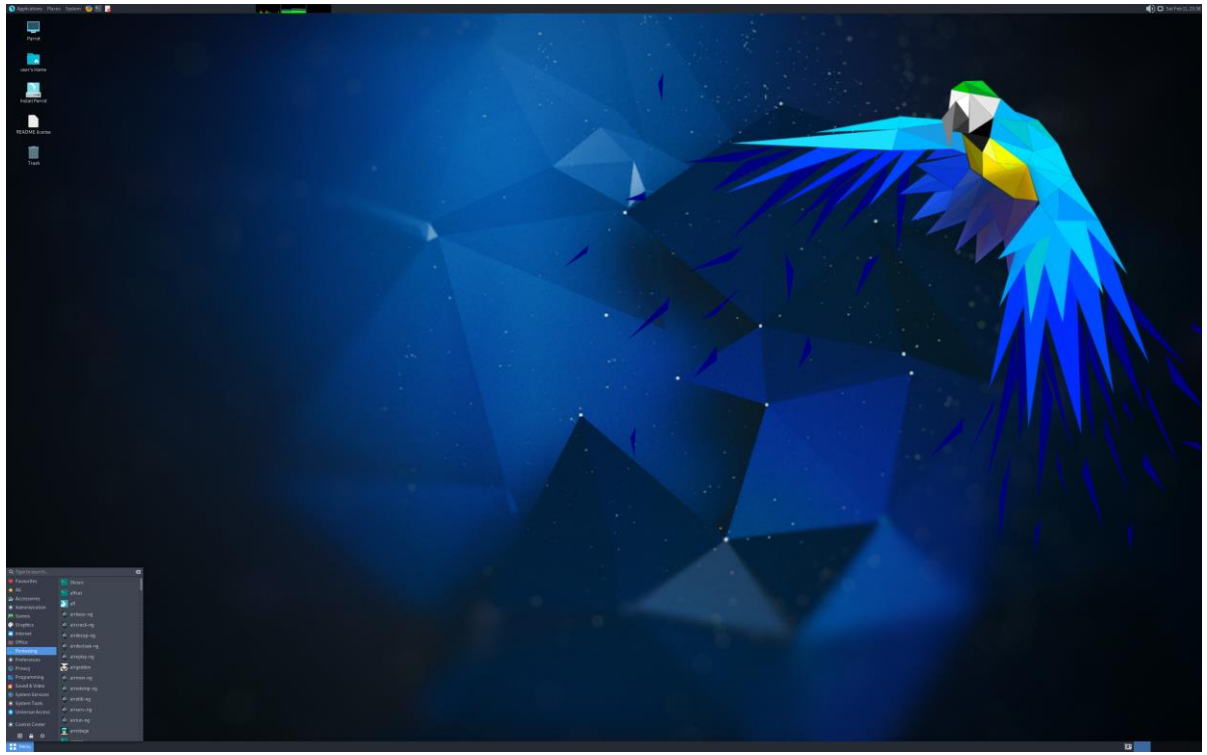
- Verschiedene Versionen von PALADIN
  - EDGE-Version ist kostenlos nutzbar
  - PALADIN PRO als vorkonfigurierter USB-Stick

→ Einfachste Distribution für schnelle Datensicherung

(C) 04.07.2023 Hochschule Mittweida

Parrot OS

- Abkömmling von Kali Linux
- Fokus:
  - Pentesting
  - Network Security
  - Forensik
- Herkunft: Italien
- Grundlage: Debian
- Weniger Kompatibel mit verschiedenen Architekturen als Kali



(C) 04.07.2023 Hochschule Mittweida

Parrot OS

- Breites Spektrum an Anwendungen:
  - Forensik
  - Reverse Engineering
  - Hacking
  - Anonymität
  - Kryptografie

- Hauptfokus liegt allerdings weniger auf Live-Anwendung
  - Eher auf der festen Installation
  - Ist aber auch per Live-Medium mit Datensicherungstools verwendbar

Weitere Live-Distros

Außerhalb der Forensik

Weitere Live-Distros

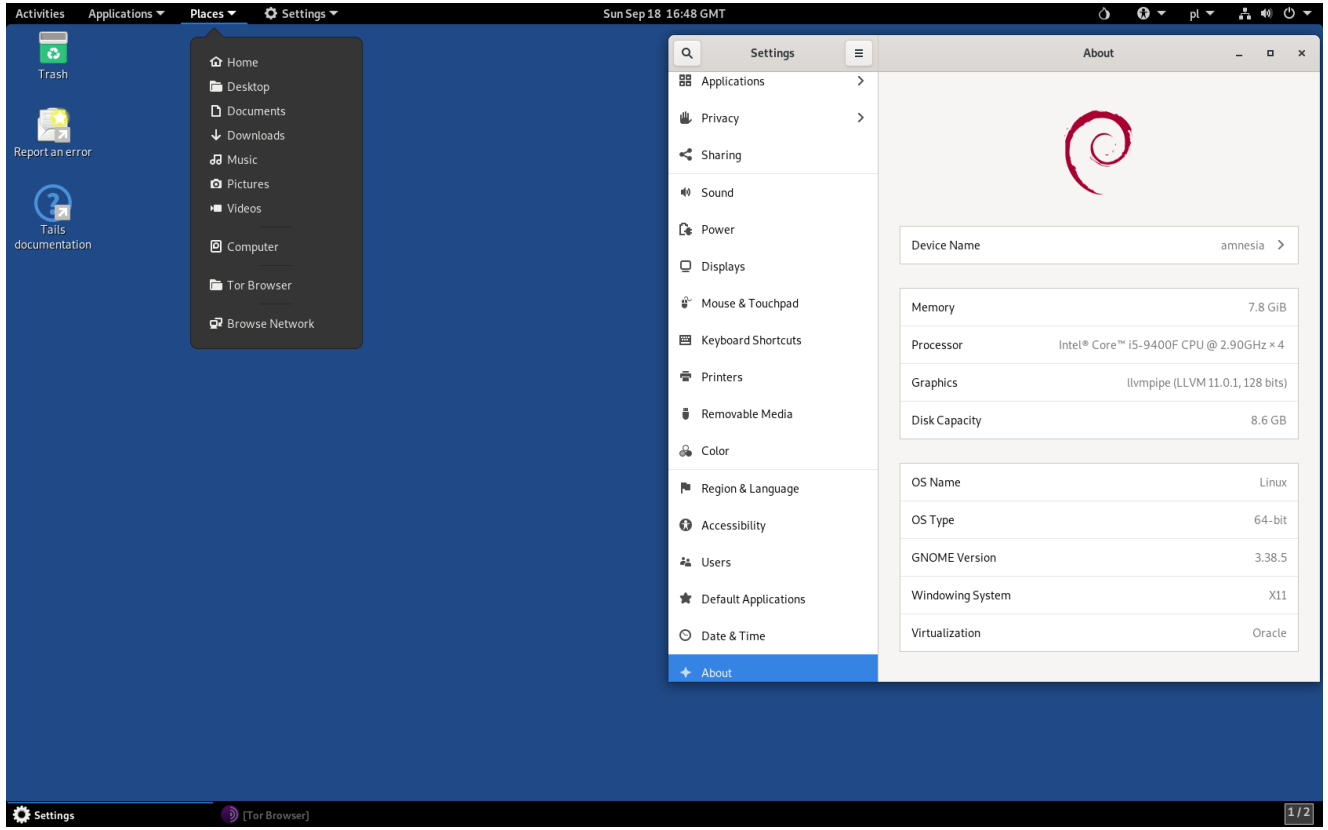
- Viele weitere Live-Versionen von bereits bekannten Distributionen:
  - Ubuntu
  - Lubuntu
  - Fedora
  - Mint
  - Manjaro

- Live-Versionen auch interessant im Bereich der Anonymität:
  - Tails
  - Whonix
  - Qubes OS

(C) 04.07.2023 Hochschule Mittweida

Tails

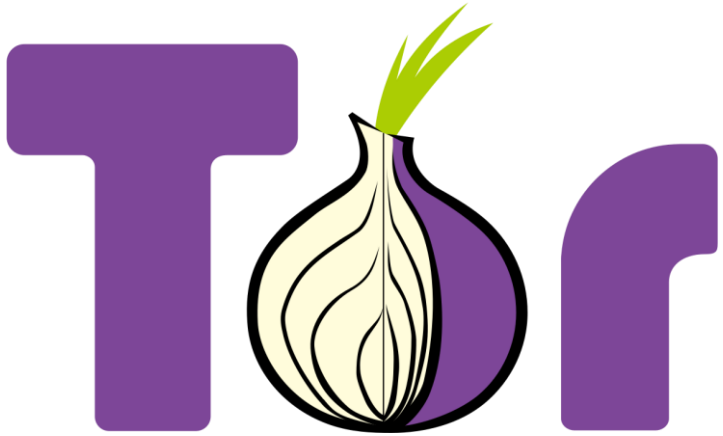
- Distribution welche nicht fest installiert werden kann
- Fokus:
  - Anonymisierung
  - Privacy
- Herkunft: Irland
- Grundlage: Debian
- https://tails.boum.org/



(C) 04.07.2023 Hochschule Mittweida

Tails

- Empfehlung der Entwickler
  - Betrieb des BS als Live Medium
  - Keine Spuren am zugrundeliegenden System
- Alternative:
  - Betrieb in VM
  - Kann teils Spuren auf dem Host-BS hinterlassen
- **Vorteile:**
  - Geht automatisch über Tor Netzwerk
  - Löscht die Daten des Nutzers bei jedem Herunterfahren
  - Keine Daten über Nutzer etc. angeben
- **Nutzen:**
  - Recherchen im Darknet etc. → auch polizeilich denkbar

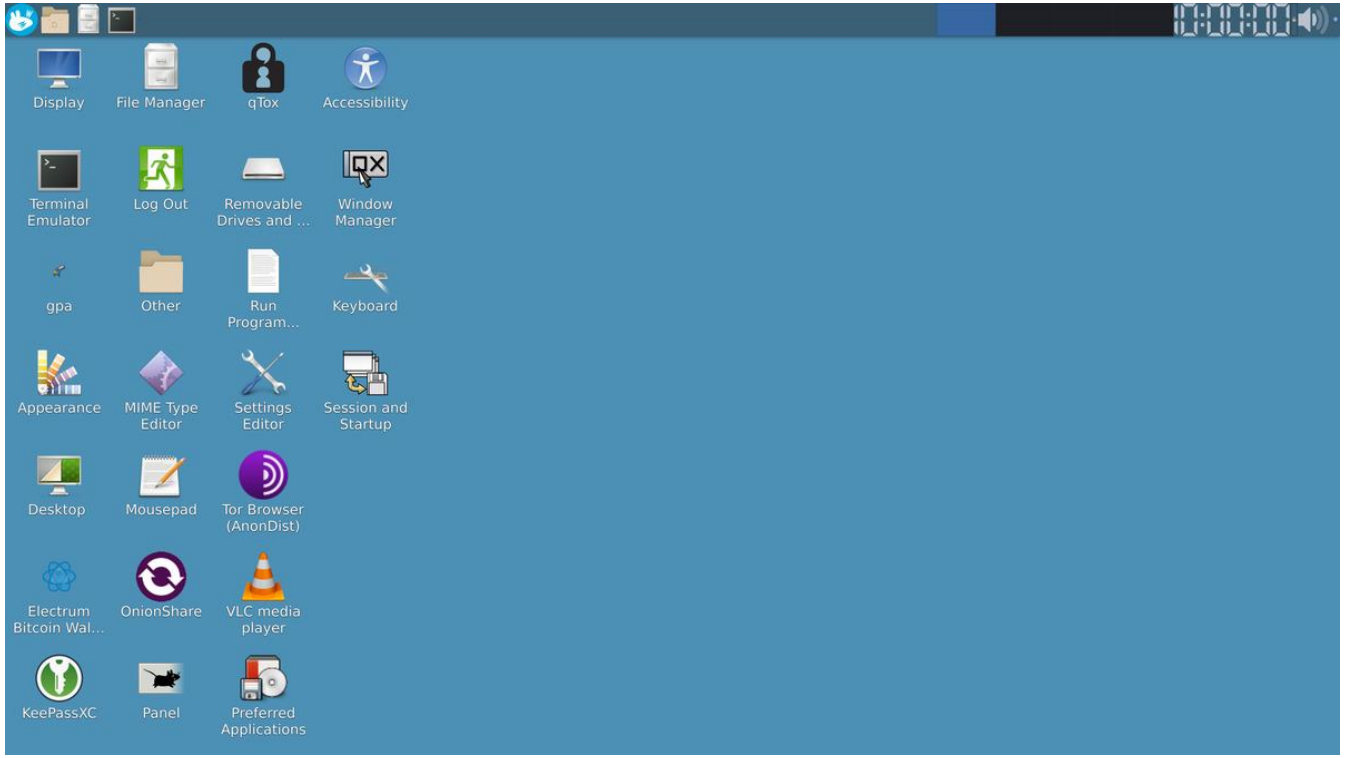


(C) 04.07.2023 Hochschule Mittweida

Whonix

Whonix

- Ebenfalls eine Distribution welche ausschließlich per Tor funktioniert
- Fokus:
  - Anonymisierung
  - Anonymer Serverbetrieb
- Herkunft: Kanada
- Grundlage: Debian



(C) 04.07.2023 Hochschule Mittweida

Whonix

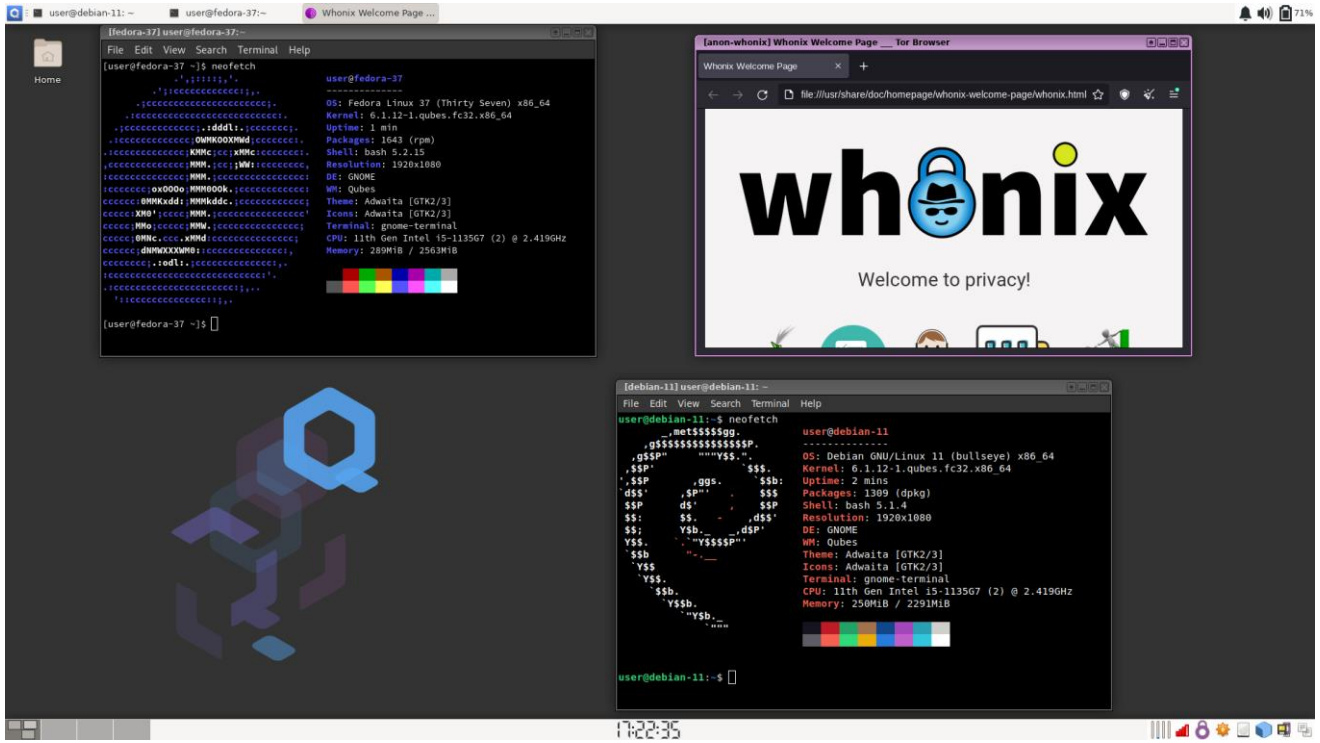
- Besteht aus zwei Teilen
  - Whonix-Gateway: Gateway ins Tor-Netzwerk
  - Whonix-Workstation: komplett isoliertes Netzwerk

- Anonymität bereit gestellter Dienste
  - Verkehr ausschließlich per Tor-Netzwerk
  - Diense anonym im Internet anbieten
  - Keine DNS-Leaks möglich
  - Selbst Root-Malware kann echte IP des Nutzers nicht herausfinden

(C) 04.07.2023 Hochschule Mittweida

Qubes OS

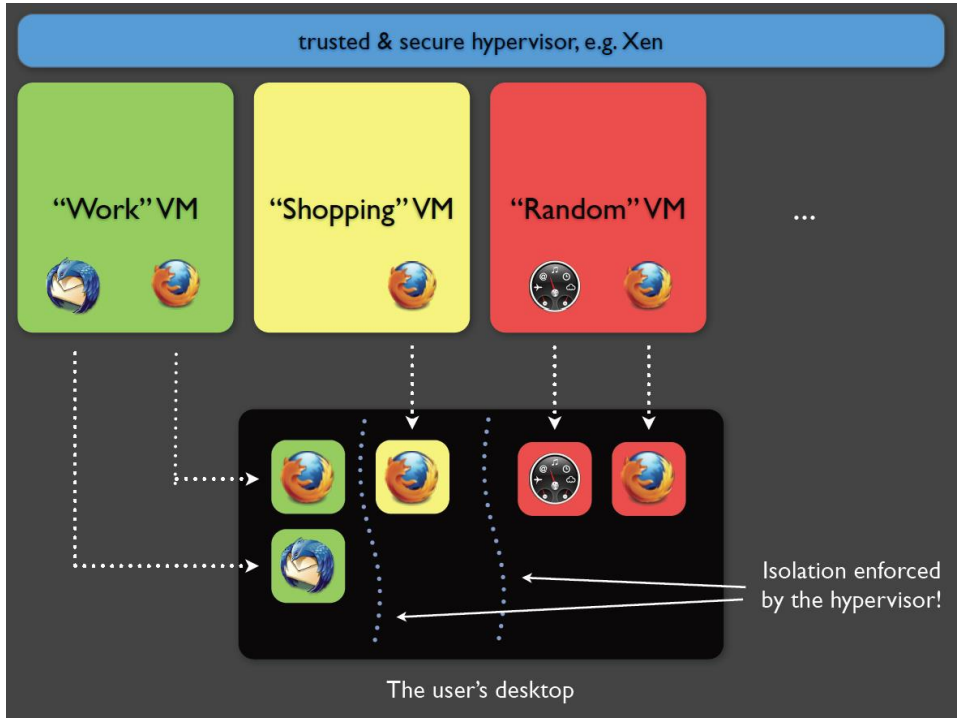
- Lässt jede Anwendung in einer separaten „Sandbox“ VM laufen
- Fokus:
  - Sicherheit durch Isolation
  - Einteilung des BS in Domänen
- Herkunft: Polen
- Grundlage: Fedora



(C) 04.07.2023 Hochschule Mittweida

Qubes OS

- Es gibt keine perfekte Sicherheit im BS
  - Kritischer Fehler begünstigt Schadsoftware
- Isolation der einzelnen Anwendungen
  - Wenn man alles auf Maschine laufen lässt, kann Schadsoftware Zugriff leicht erweitern
  - Durch Isolation kann sich Malware schwieriger ausbreiten
- Xen virtual Machines
  - Aufbau verschiedener Domänen



(C) 04.07.2023 Hochschule Mittweida

Live-Sicherung

am Beispiel von Sumuri PALADIN EDGE

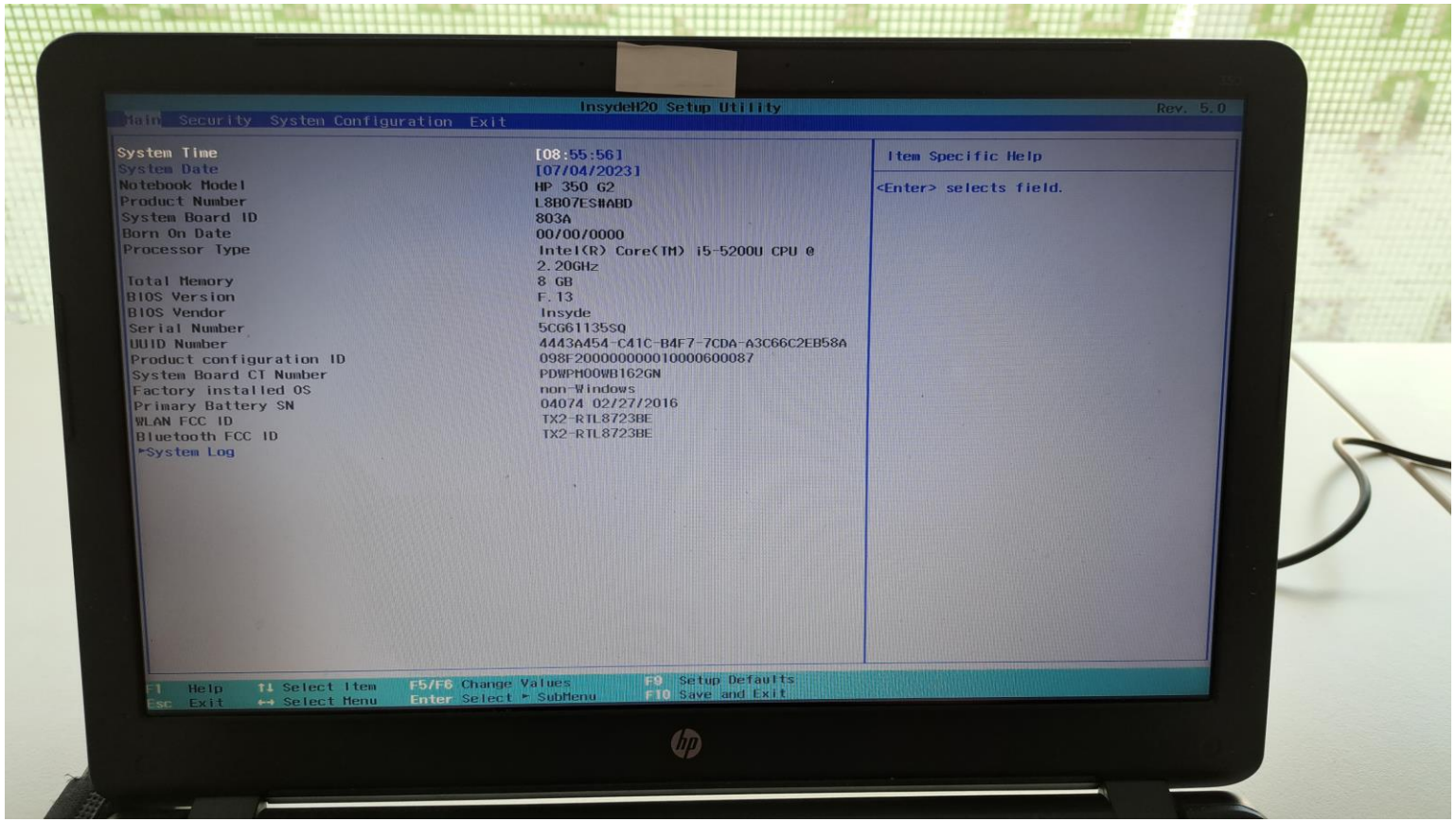
Beispielsicherung

- Folgend soll eine beispielhafte Sicherung mit PALADIN Edge an einem Laptop durchgeführt werden
- Sicherungsdetails:
  - **Gerät:** USB-Stick SanDisk Extreme Pro 128 GB
  - **Asservatennummer:** Ass_01
  - **Fallnummer:** 12345
  - **Sicherungsformat:** EWF (E01)
  - **Segmentgröße:** 2GB

(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

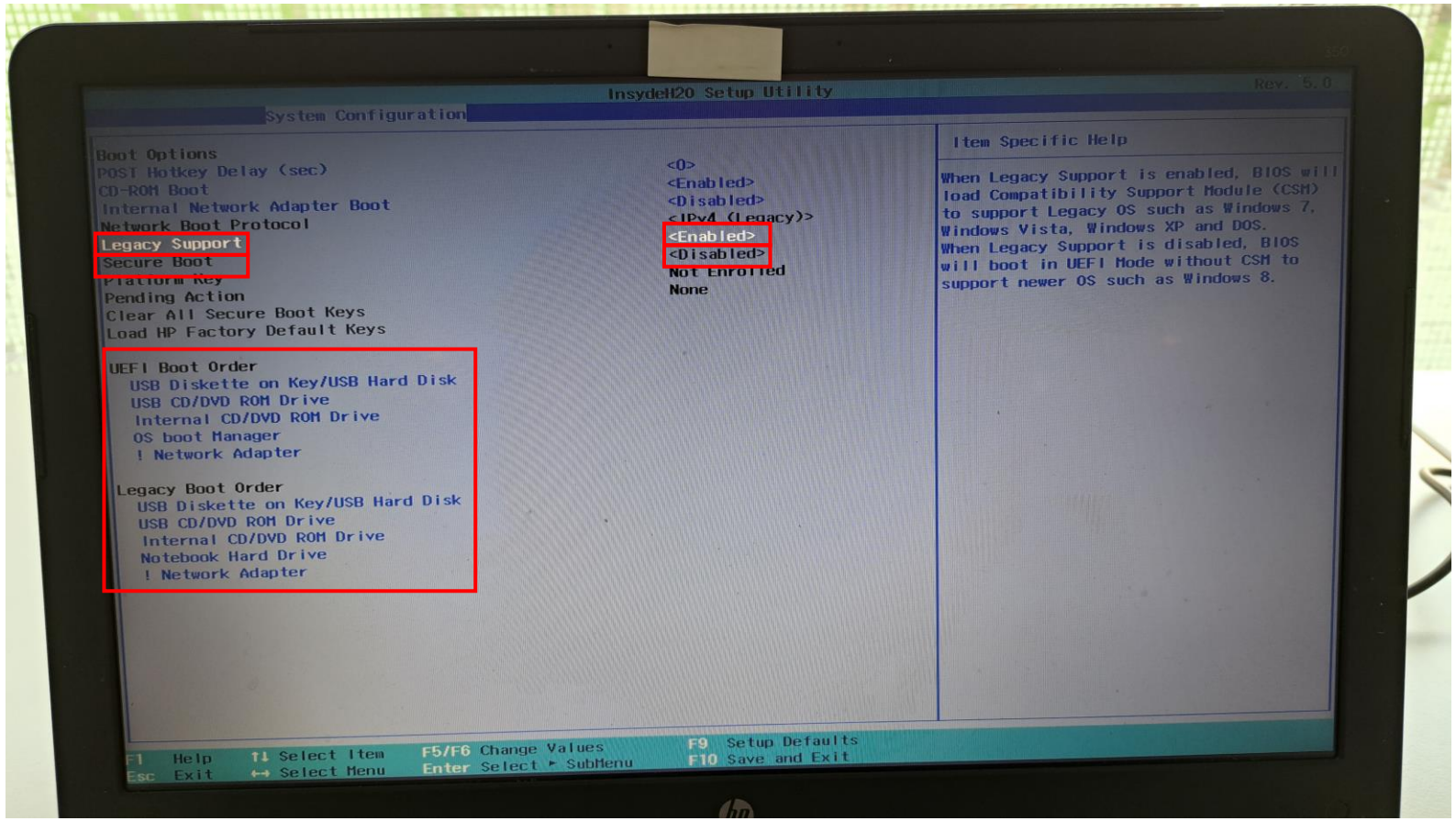
- Bootmenü öffnen → Einstellungen für Live-Boot vornehmen



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

- Legacy Boot aktivieren → Secure Boot deaktivieren → Bootreihenfolge anpassen



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

- Bootmenü verlassen → übrige Hardware anstecken

Zu sichernder Stick
128 GB

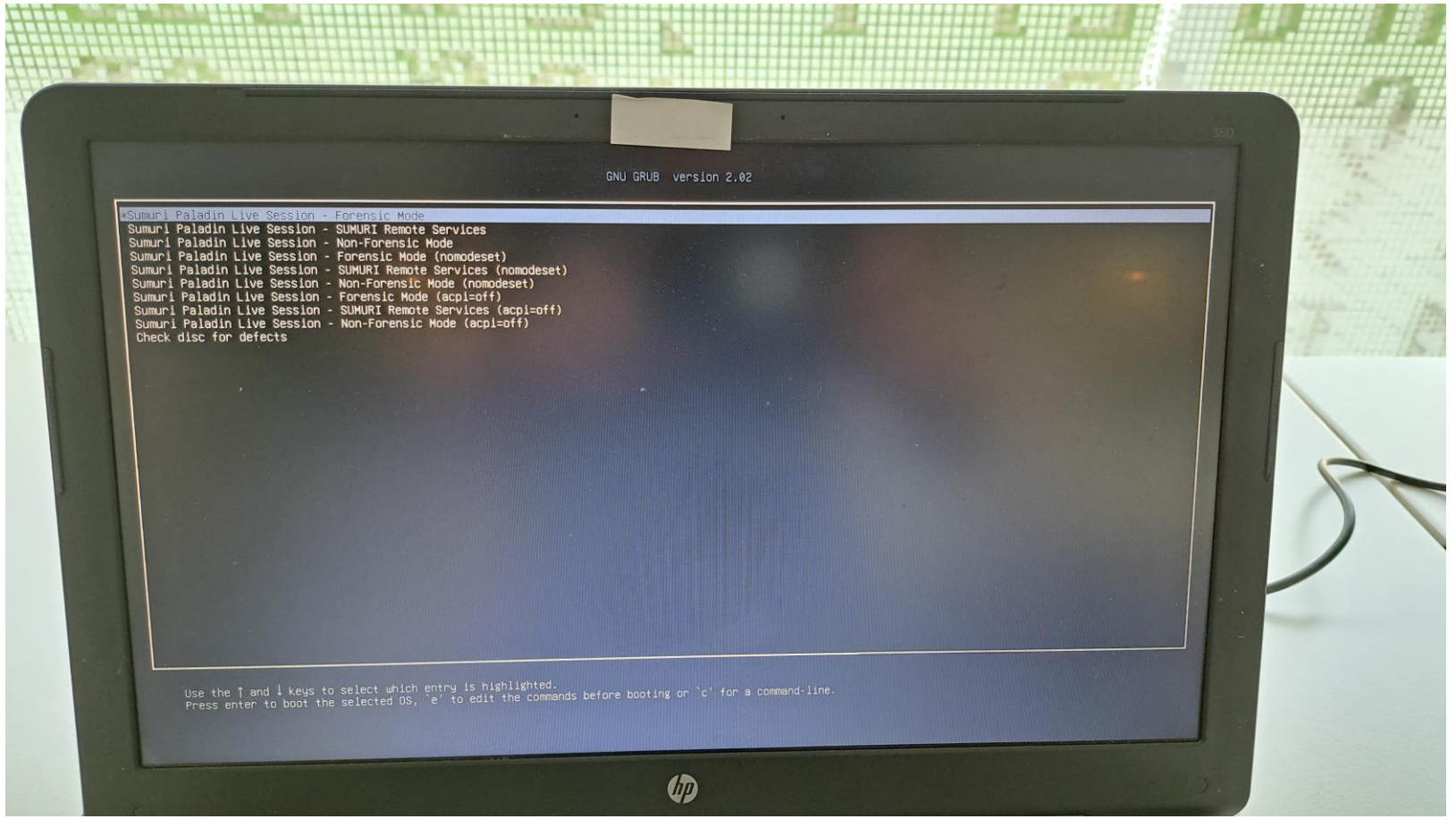
Zieldatenträger
256 GB

PALADIN Live-
Bootmedium

(C) 04.07.2023 Hochschule Mittweida

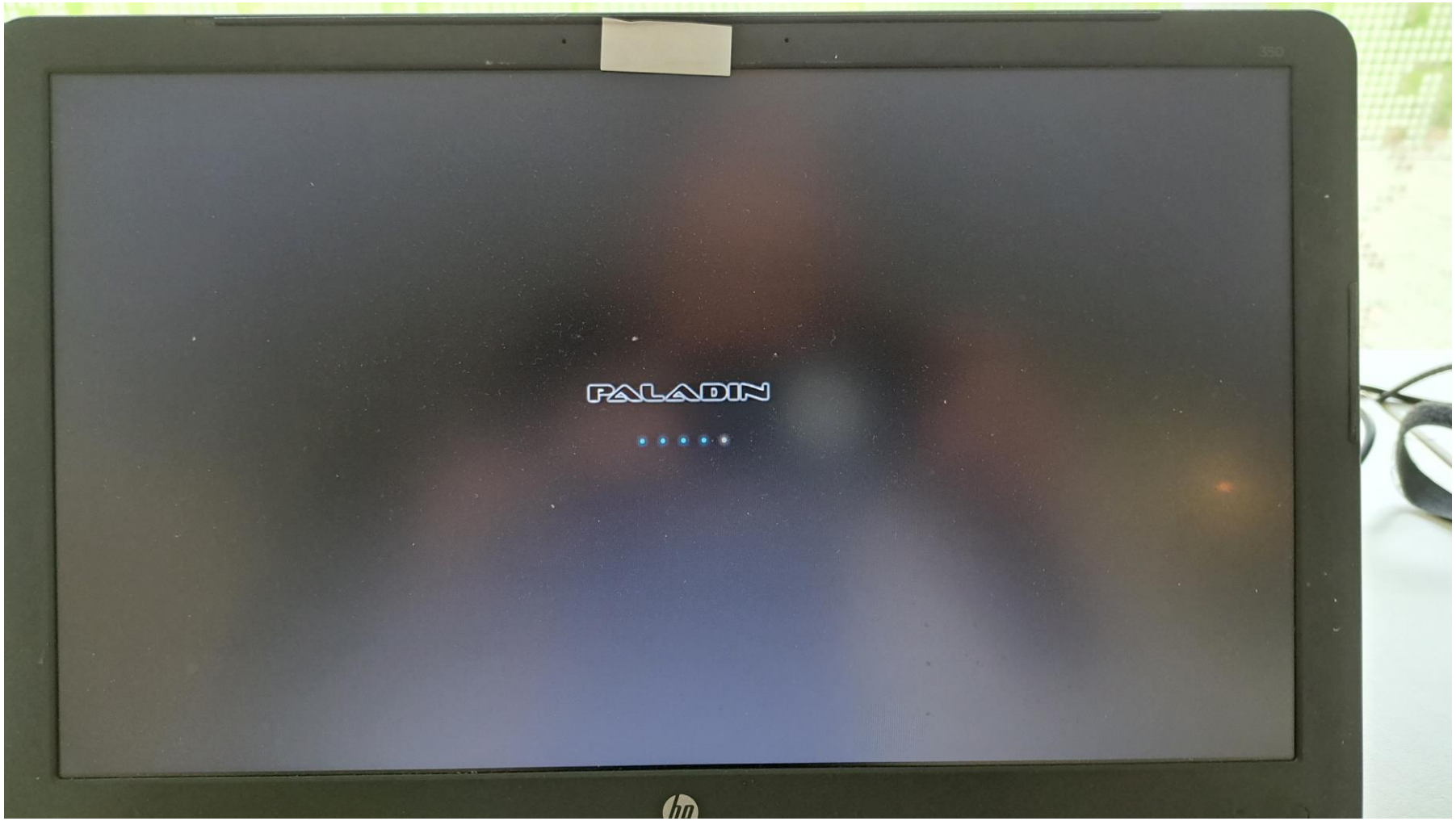
Beispielsicherung

- Starten des Rechners → Boot von PALADIN Live Bootmedium



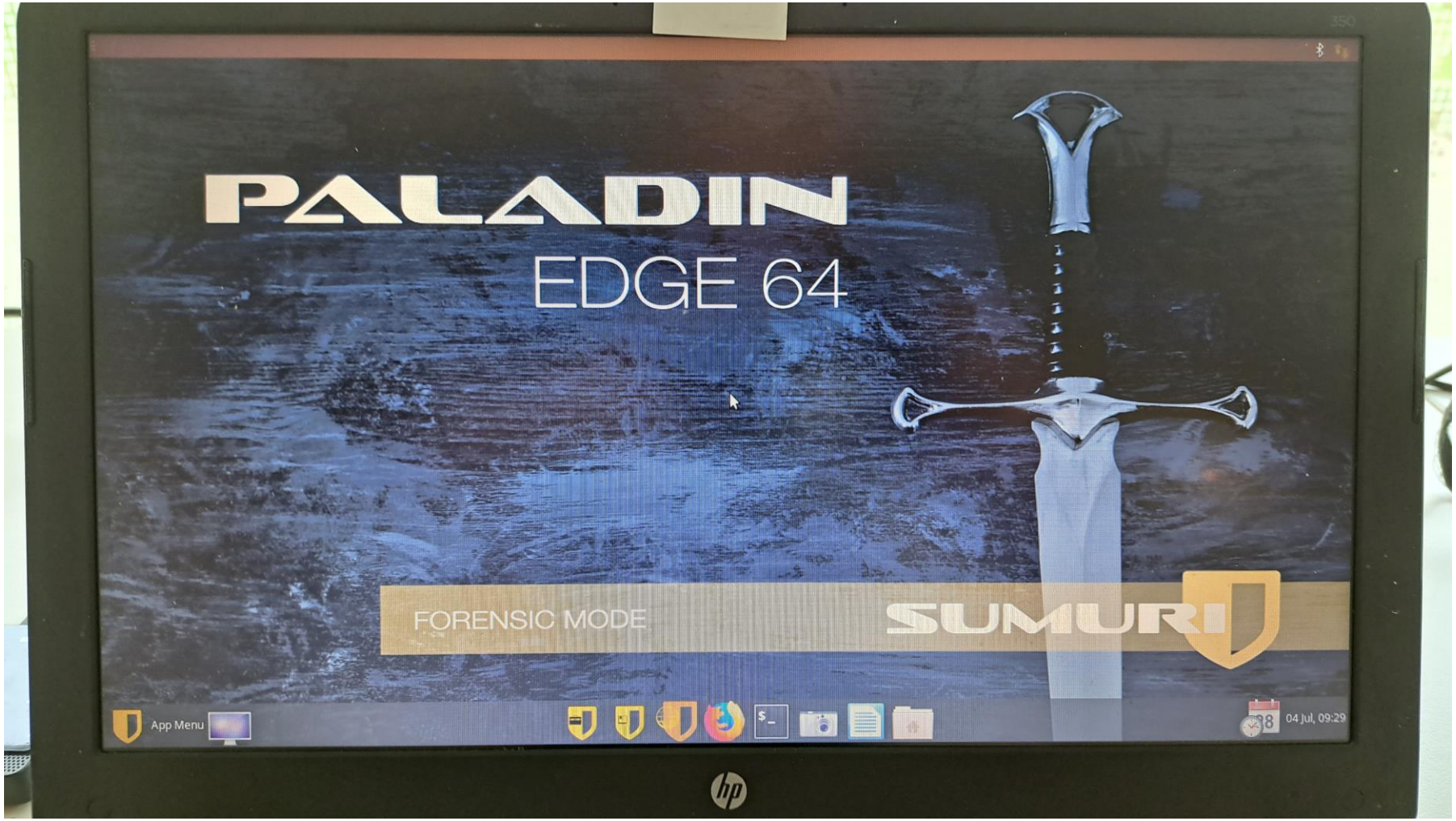
(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung



(C) 04.07.2023 Hochschule Mittweida

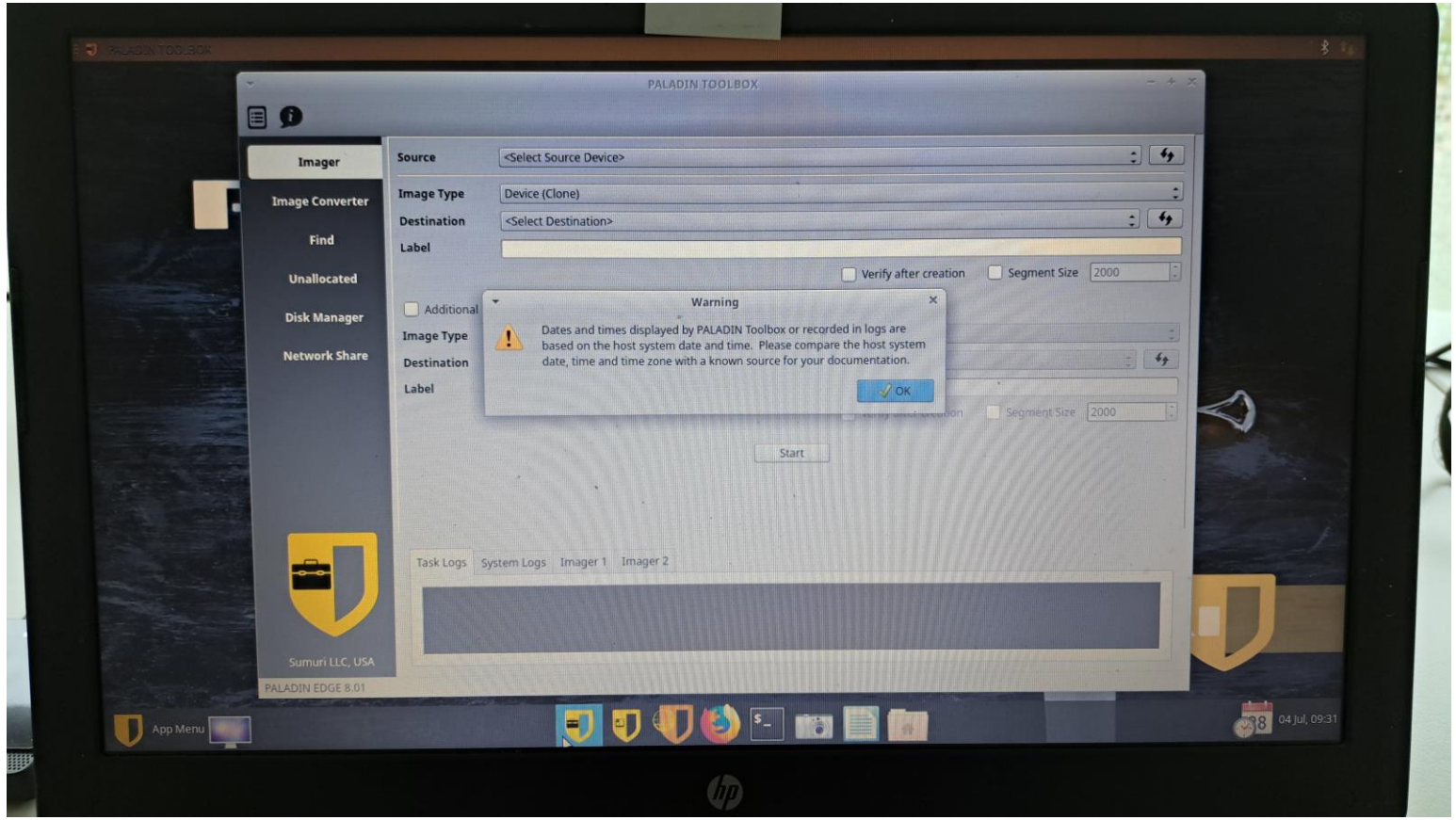
Beispielsicherung



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

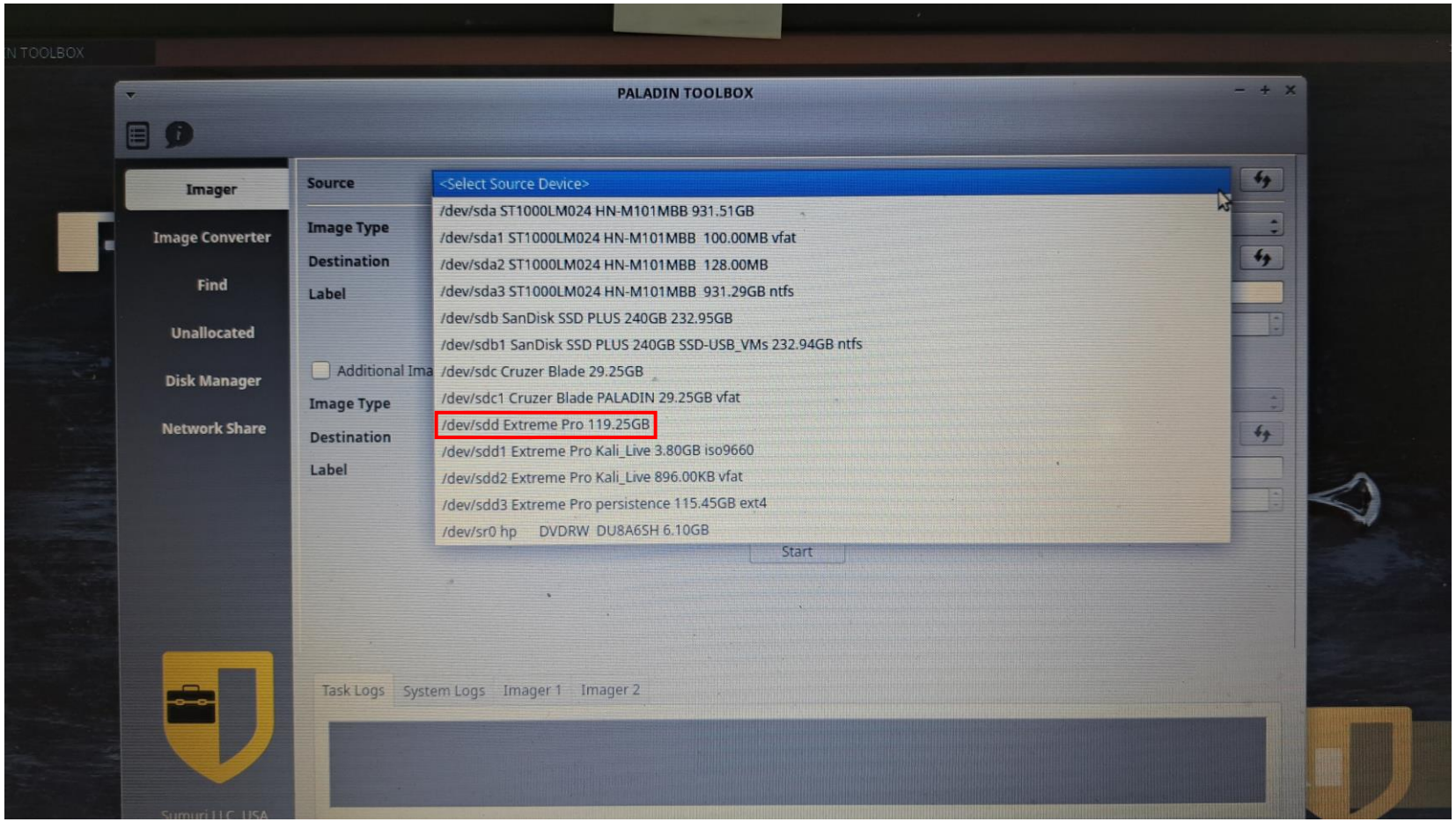
- Warnung zu unterschiedlichen Zeitangaben (Zeitunterschied beachten)



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

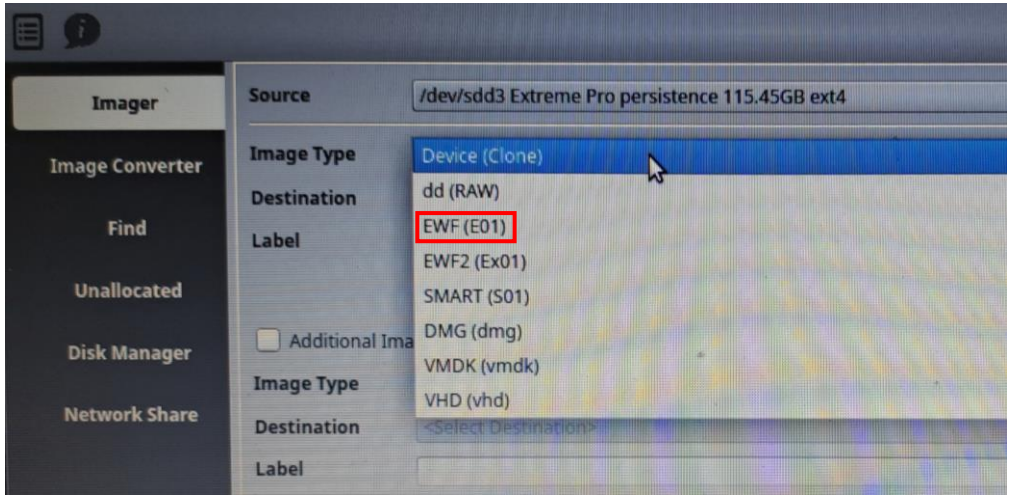
- Quelle auswählen → /dev/sdd → 4 Festplatte komplett (alle Partitionen)

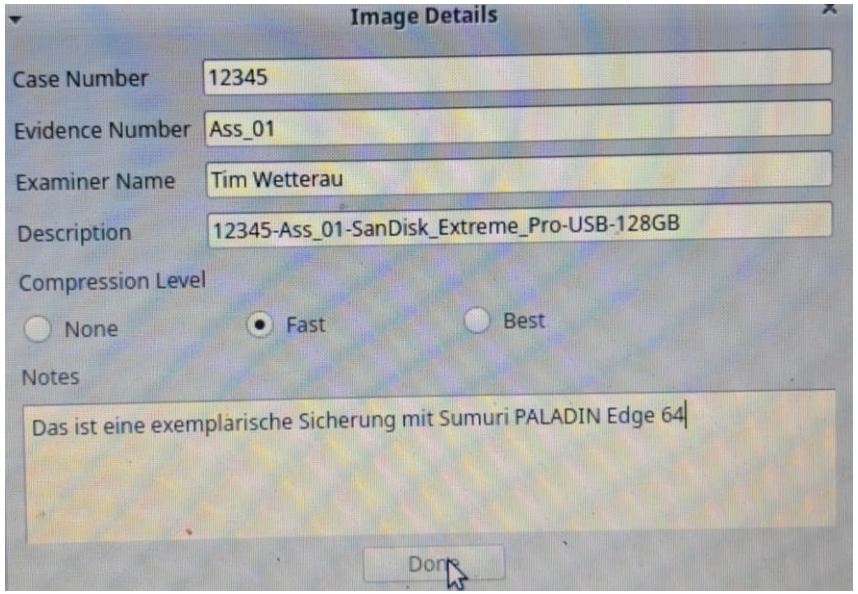


(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

- Zielformat auswählen
- Falldaten eingeben

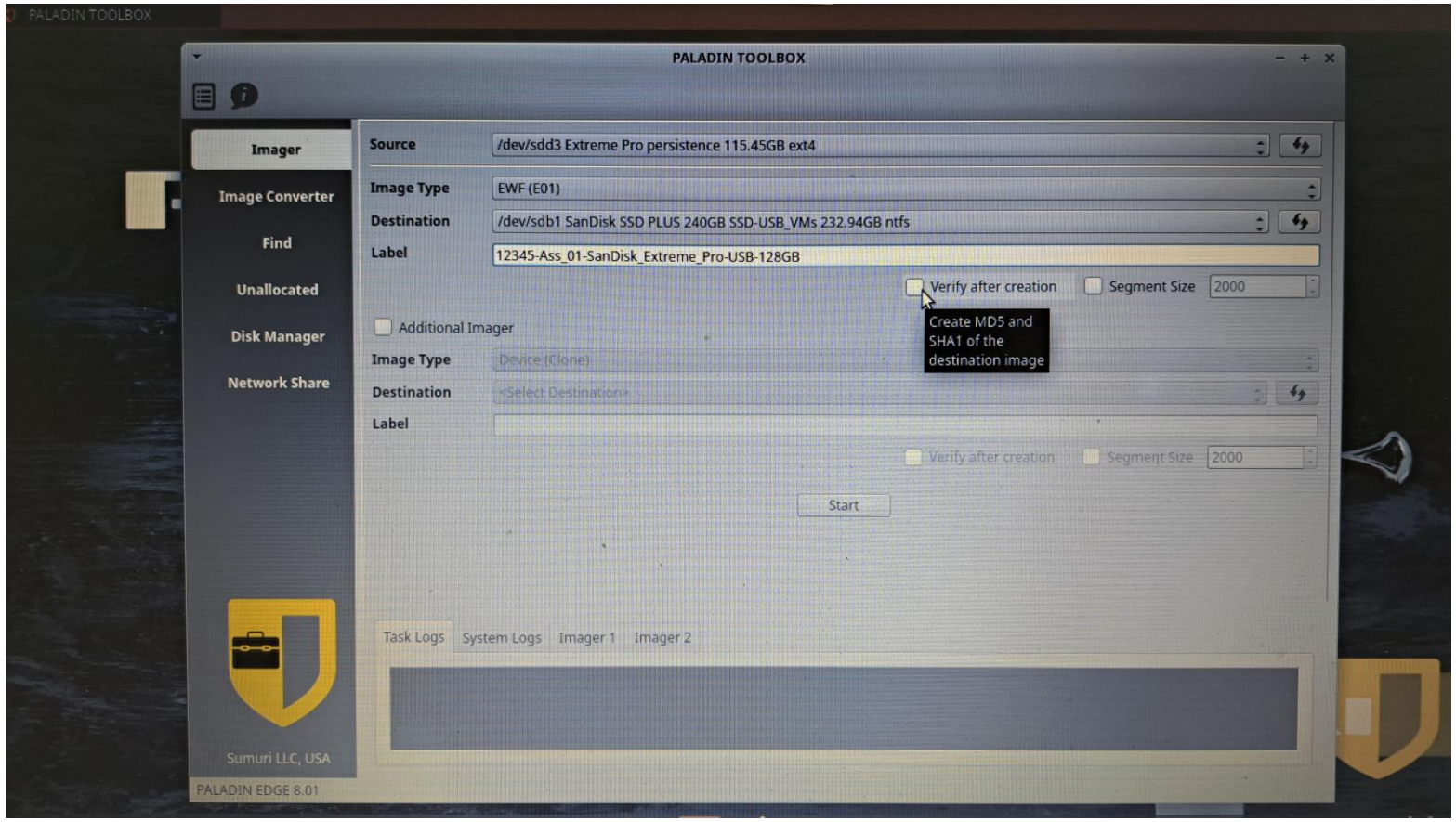




(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

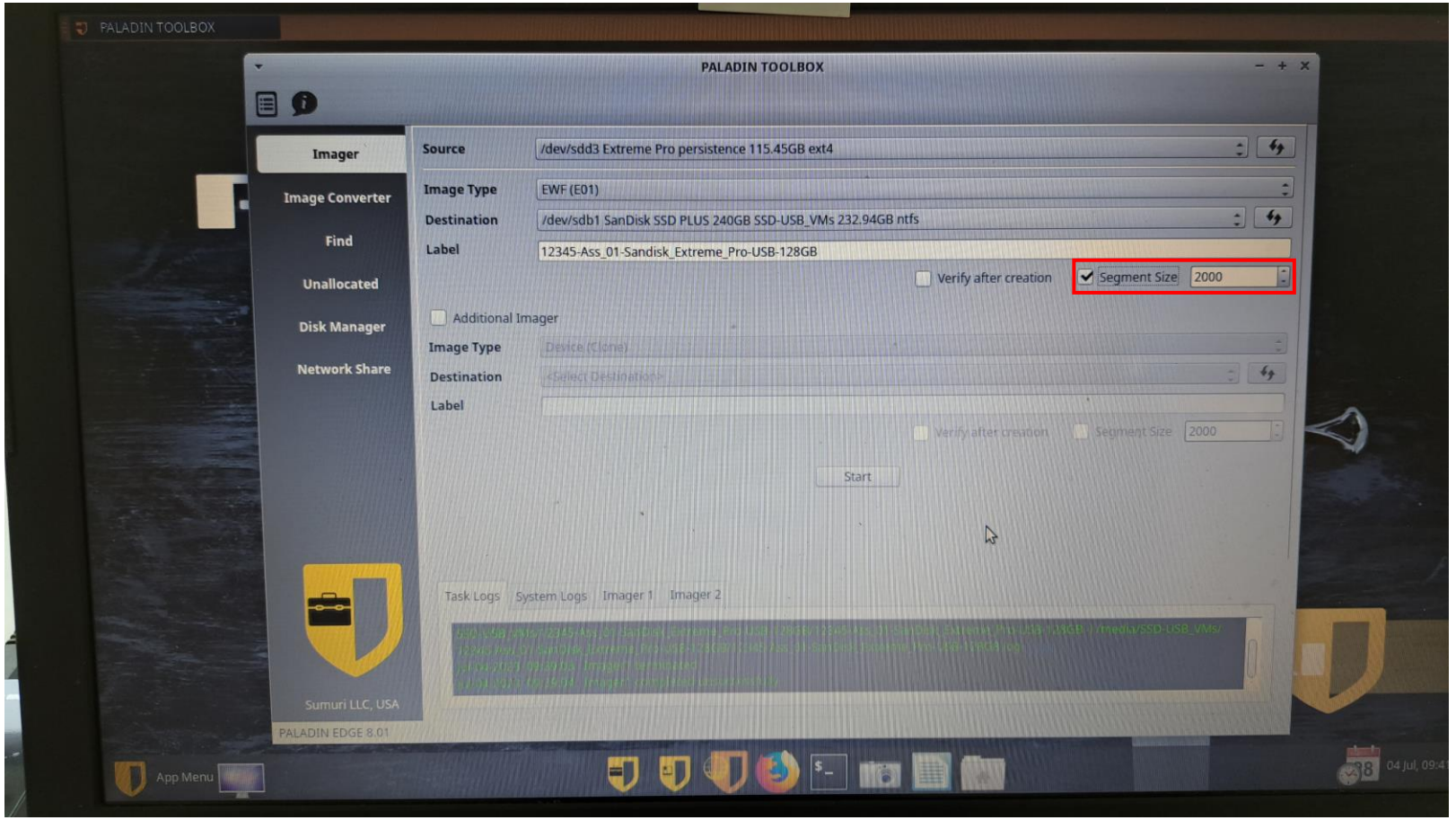
- Optional: Hashsumme über gesicherten Datenbestand abgleichen



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

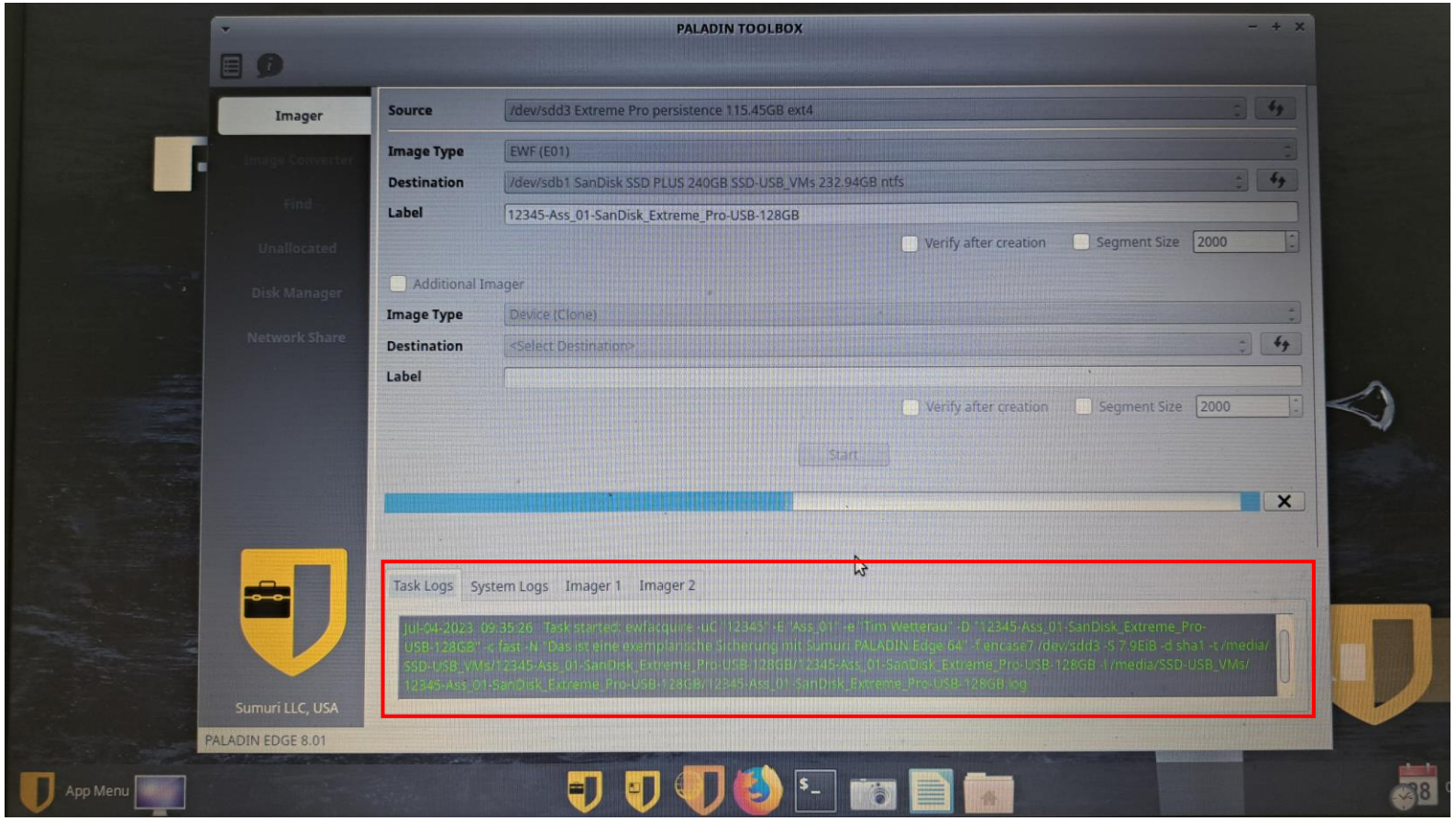
- Segmentgröße festlegen (2 GB = 2000 MB)



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

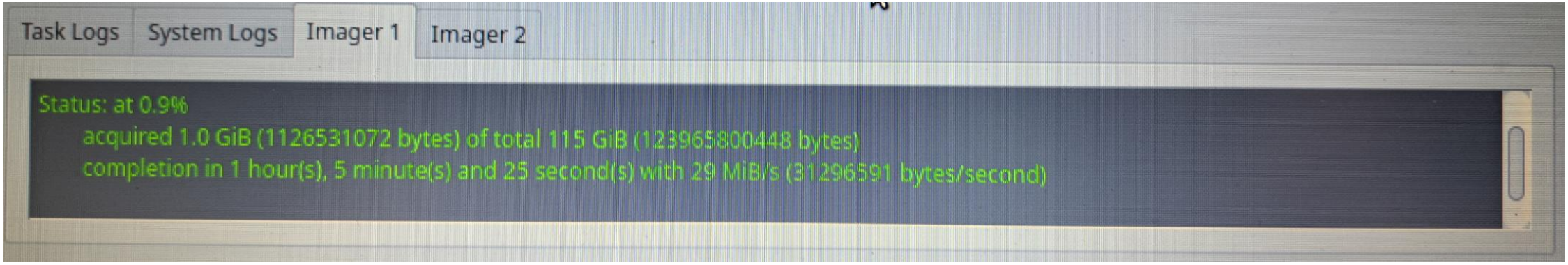
- Start der Sicherung → Task Logs → Informationsanzeige



(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

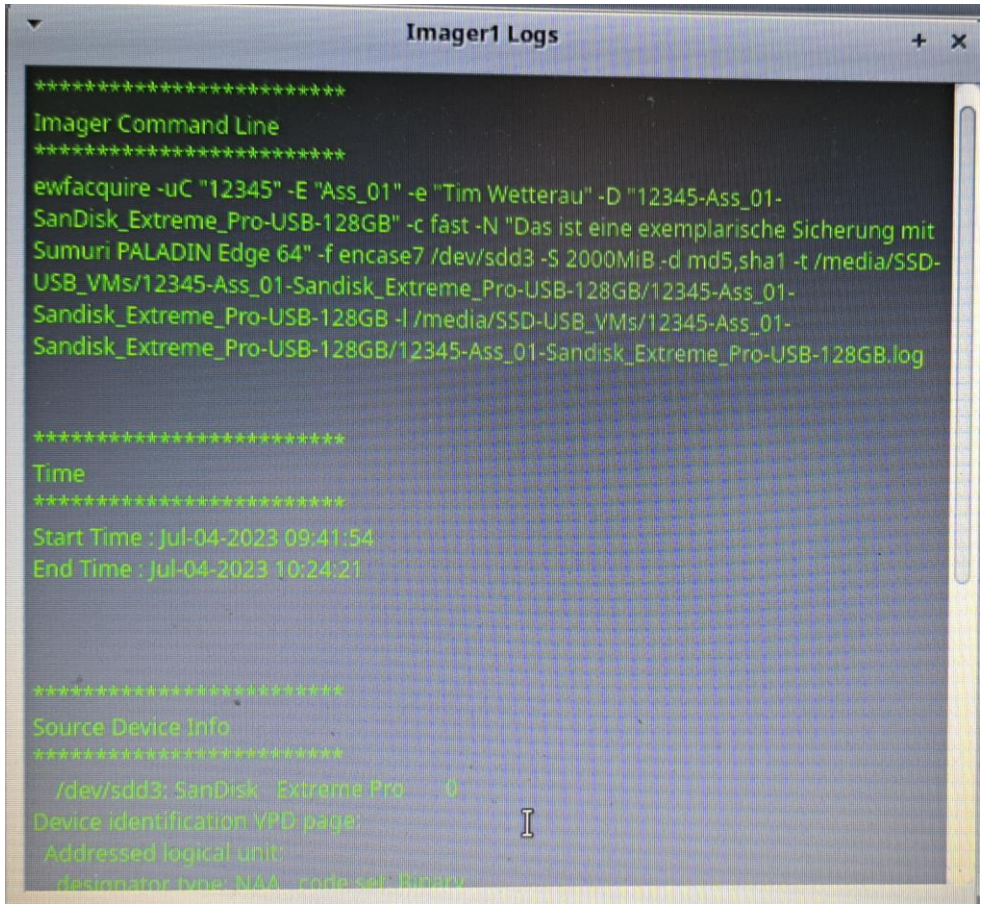
- Fortschrittsanzeige der Sicherung (Zeitabschätzung)



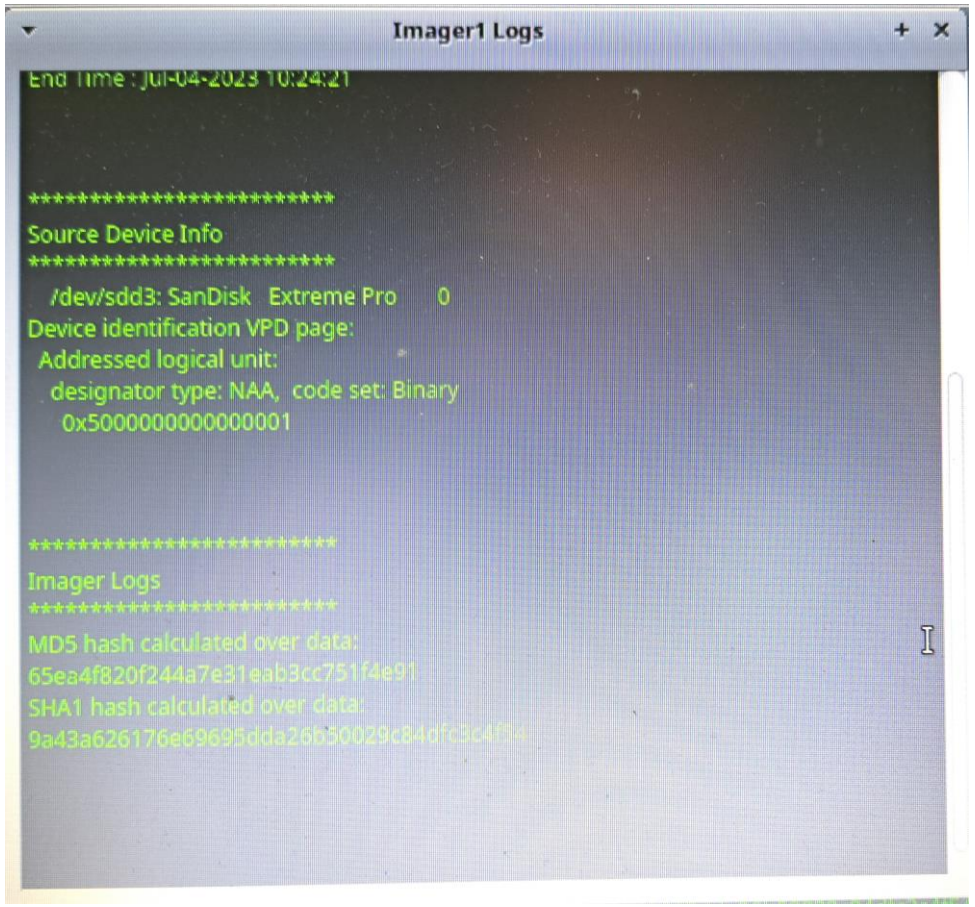
(C) 04.07.2023 Hochschule Mittweida

Beispielsicherung

- Anzeige Sicherungslog



- Anzeige Hashsumme



(C) 04.07.2023 Hochschule Mittweida

Zusammenfassung

Zusammenfassung

Wir haben in dieser Vorlesung folgende Inhalte beleuchtet:

- Warum bietet es sich an Live-Distributionen zu nutzen und haben gesehen, welche Ziele verfolgt werden können
- Wir haben eine kleine Auswahl an Distributionen kennengelernt, welche Live verwendet werden können. Außerdem ist uns nun bekannt, worauf sich die einzelnen Distros fokussieren.
- Letztlich haben wir uns exemplarisch eine Sicherung mit PALADIN Live angesehen und einen USB-Stick gesichert.

(C) 04.07.2023 Hochschule Mittweida

Vielen Dank

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Prof. Ronny Bodach

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

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
@ bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau| Raum 8-205
Am Schwanenteich 6b| 09648 Mittweida

Tim Wetterau B.Sc., Leander Hoßfeld B.Sc.

T +49 (0) 3727 58-1752
+49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de
hossfeld@hs-mittweida.de

Haus 6 | Grunert de Jacome Bau | Raum 6-031
Am Schwanenteich 4b | 09648 Mittweida

hs-mittweida.de