Kali Linux

Inhalt

[Download auf VMware 1](#_Toc138779914)

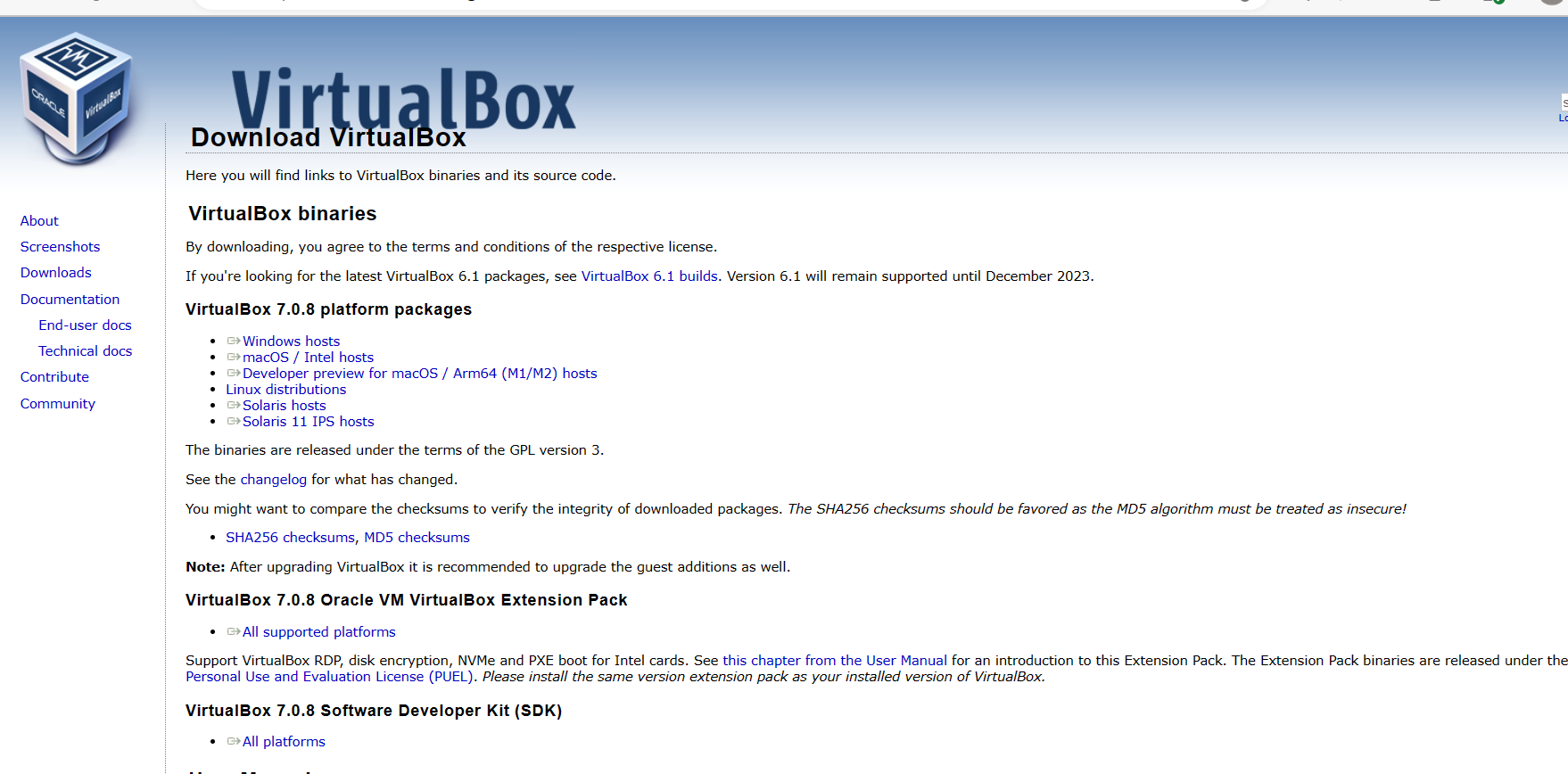
[Download auf USB-Stick 4](#_Toc138779915)

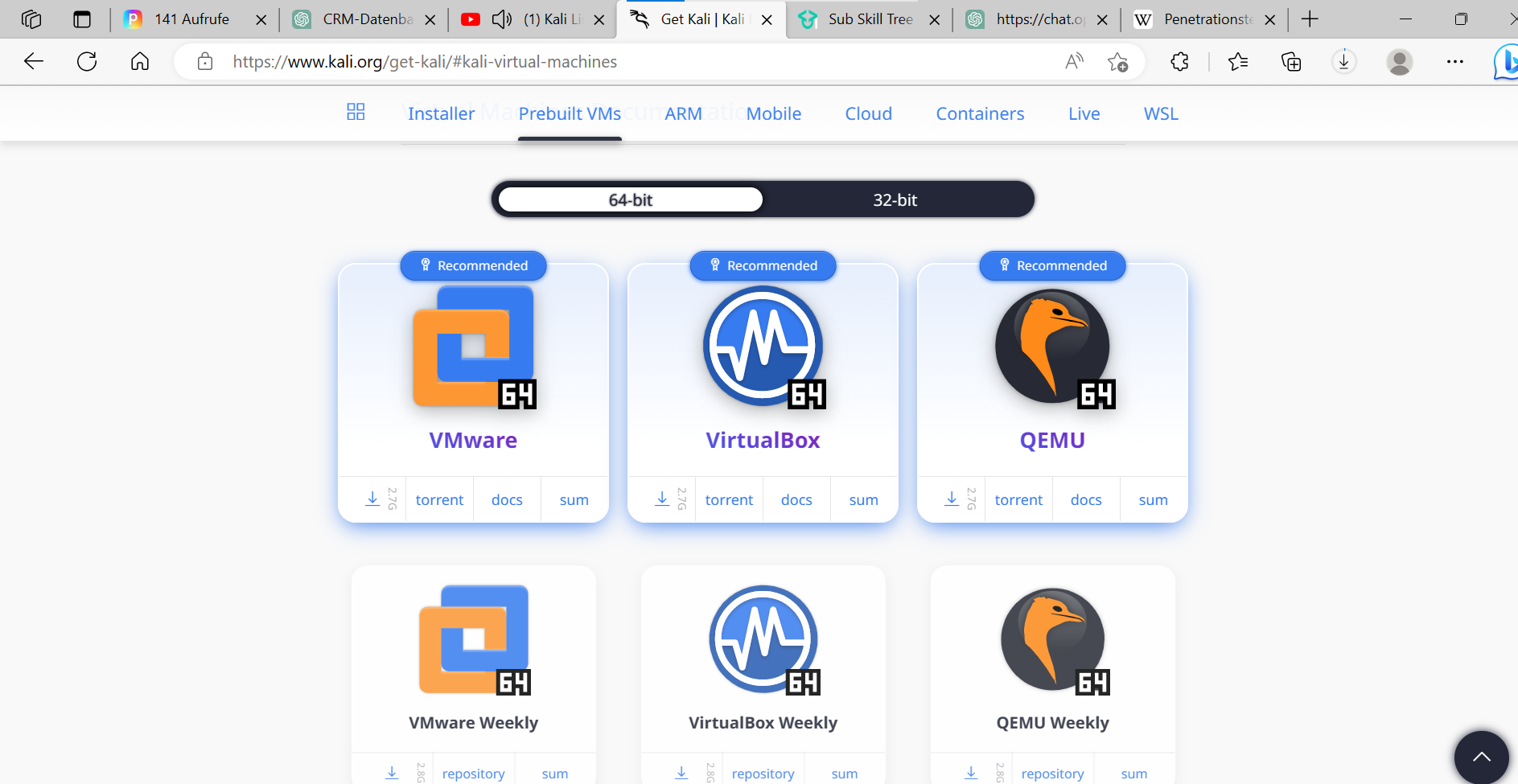
[Terminal Übungen 13](#_Toc138779916)

[Wlan Passwort knacken 16](#_Toc138779917)

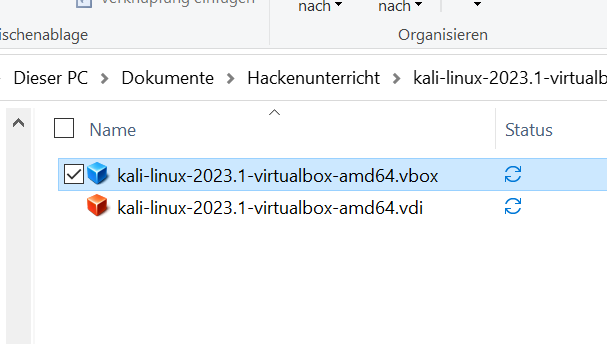
# Download auf VMware

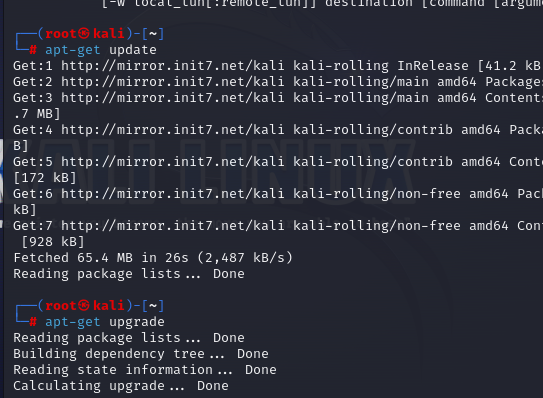
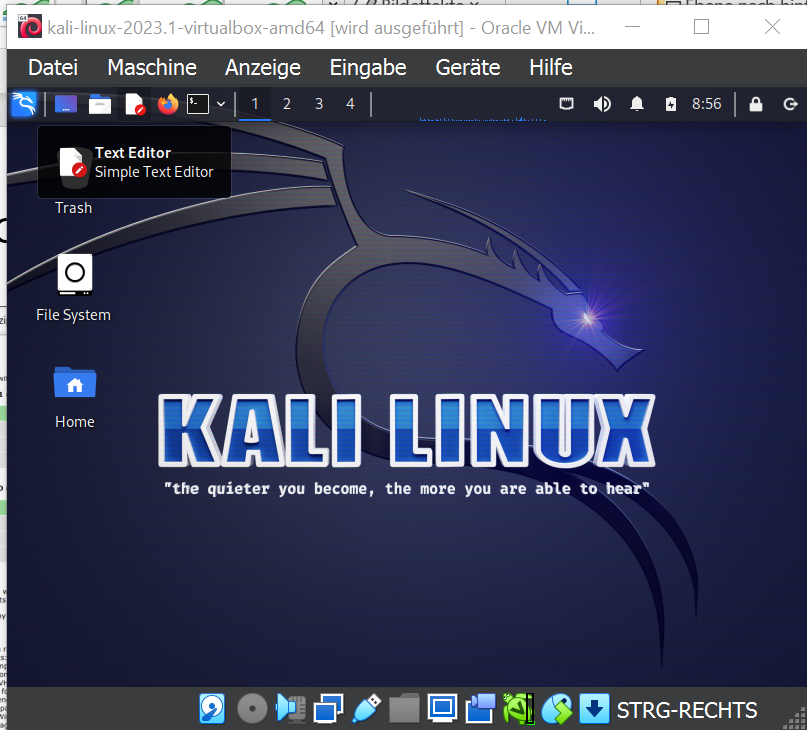
Quelle: [(51) Kali Linux in Virtualbox installieren 2020 - als virtuelle Maschine: die einfache Variante - YouTube](https://www.youtube.com/watch?v=9lmGxgq7O1Q&t=313s&ab_channel=TheMorpheusTutorials)

1. Als erstes habe ich Virtual Box heruntergeladen. 
2. Danach die Kali Linux. vbox Datei welche als Disk fungiert beim Booten.



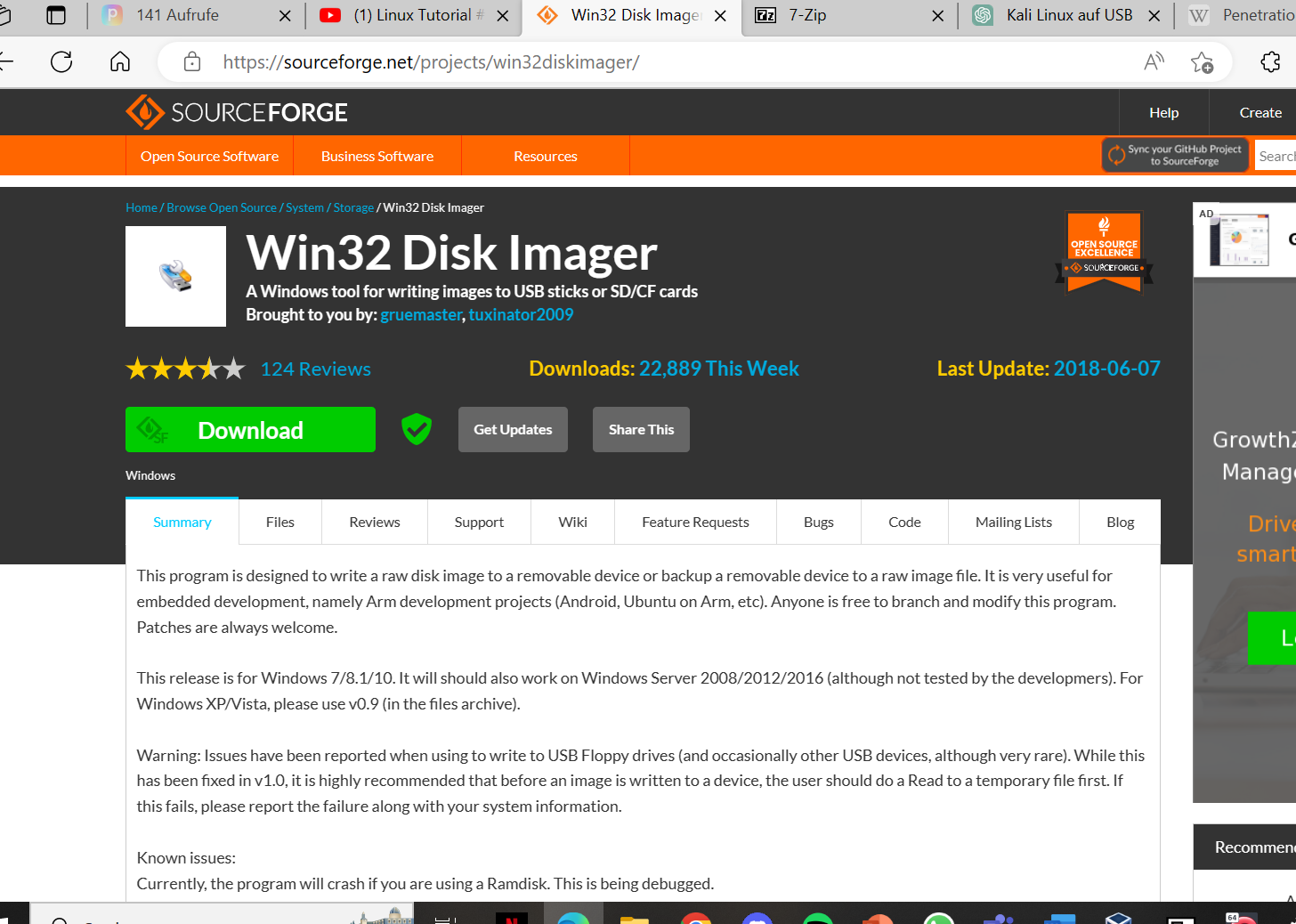
1. .vbox datei durchführen und es wird automatisch in Virtual Box initialisiert

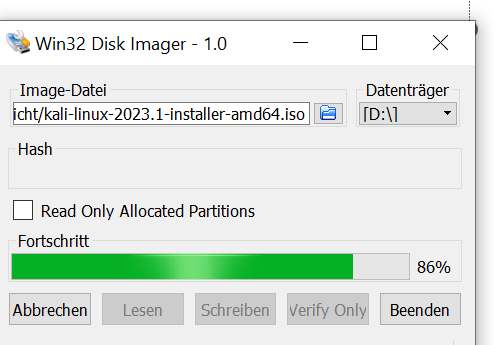
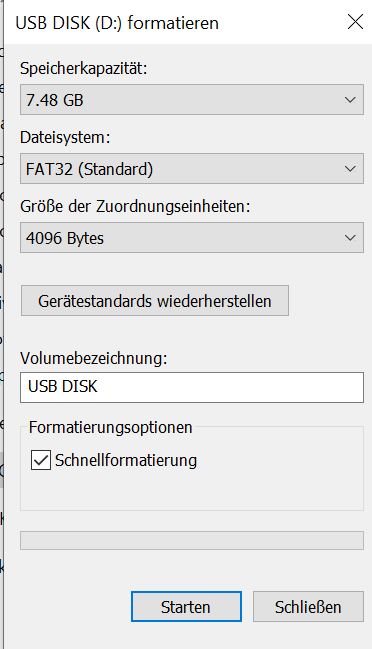


1. Kali Linux erfolgreich auf VMware Installiert und gebootet

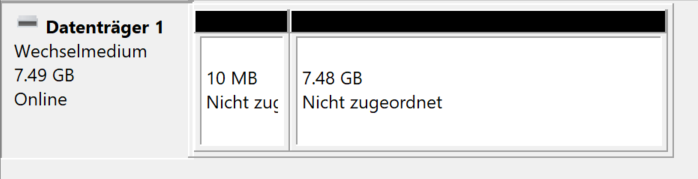
# Download auf USB-Stick

Quelle: [(51) Linux Tutorial #0.1 - Linux auf USB installieren, VirtualBox von USB starten - YouTube](https://www.youtube.com/watch?v=Gg0suugWa4E&t=328s&ab_channel=TheMorpheusTutorials)





Systemsteuerung/Verwaltung/Computerverwaltung/Datenträgerverwaltung/



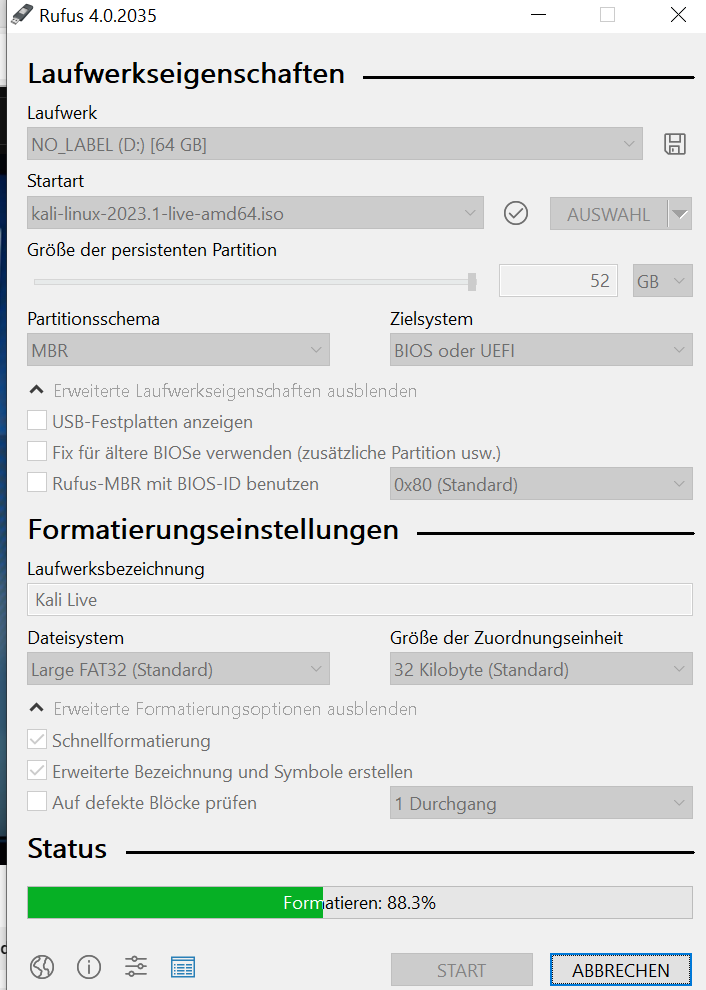
Nummer des Datenträgers merken

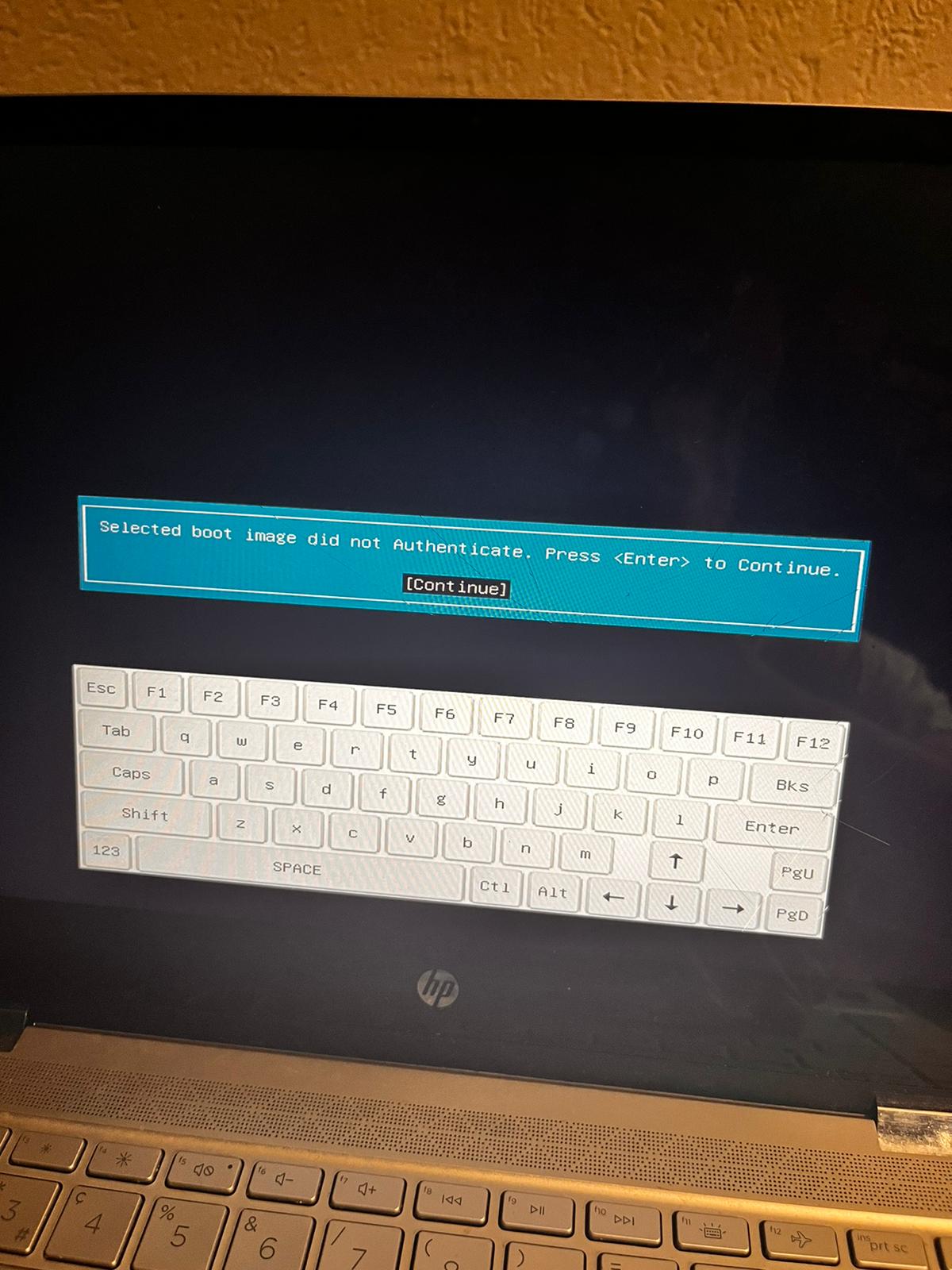
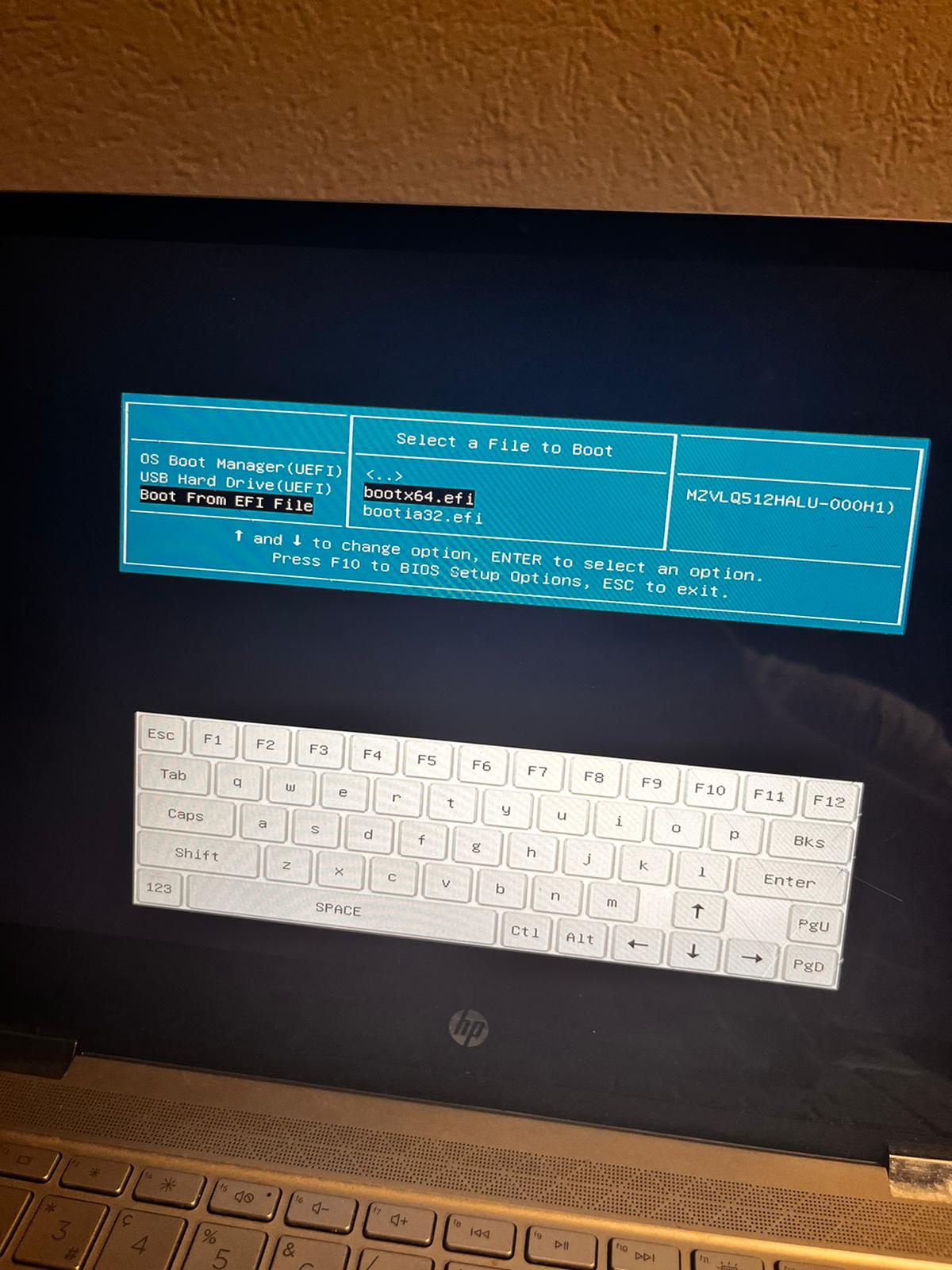
VBoxManage internalcommands createrawvmdk -filename D:\Tuts\Kali\Kaliusb.vmdk -rawdisk [\\.\PhysicalDrive1](file:///\\.\PhysicalDrive1)

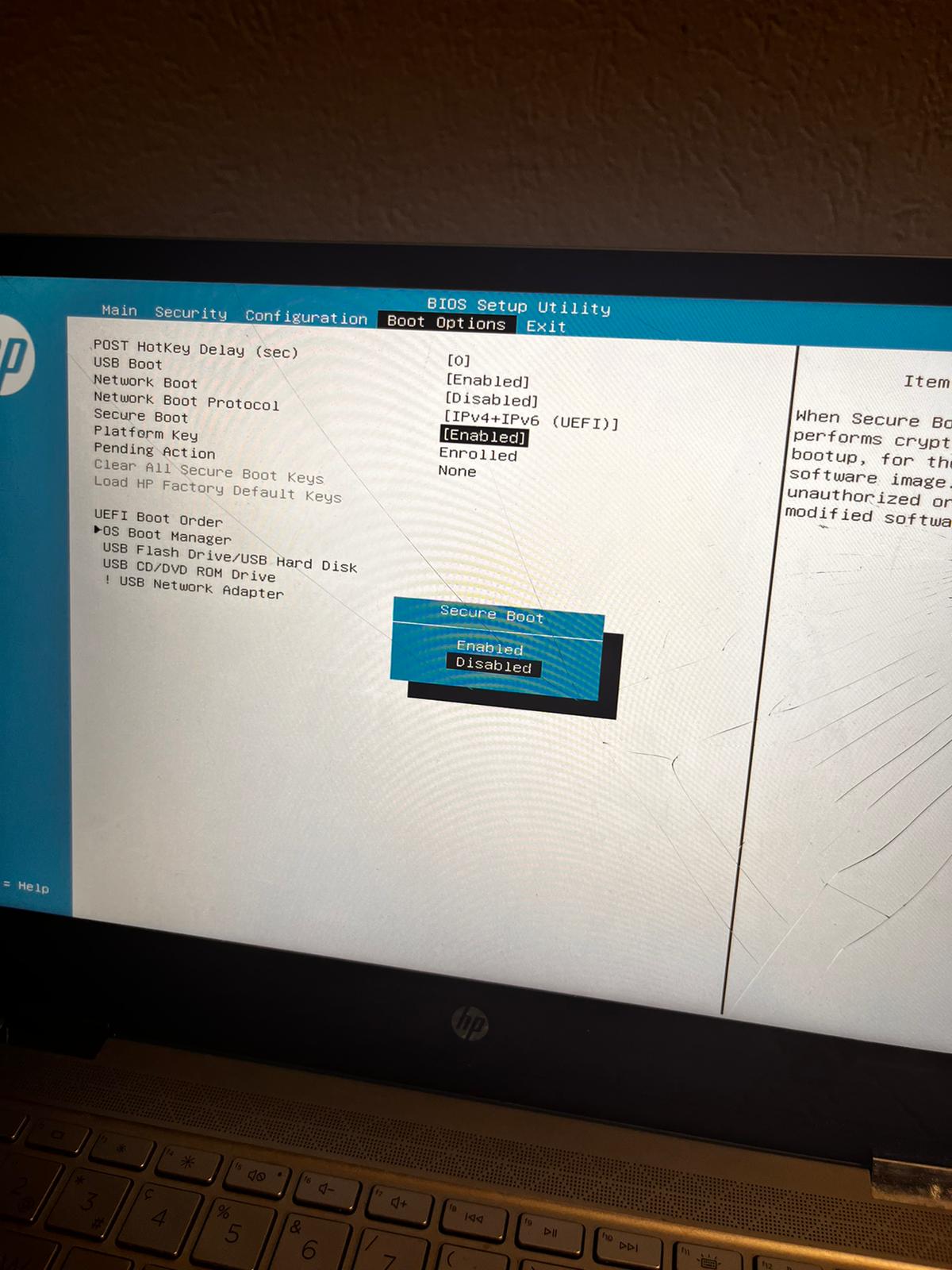
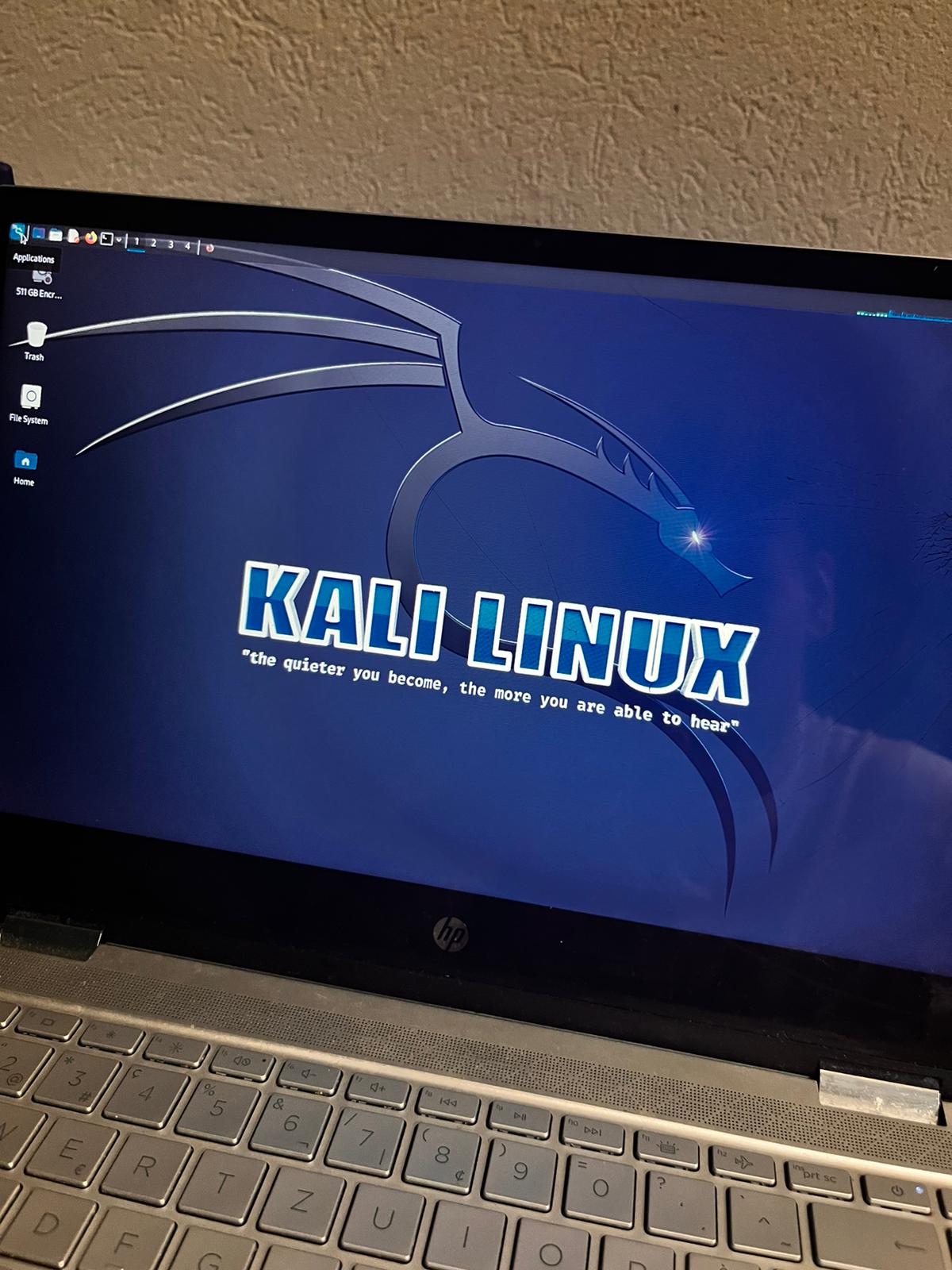
Fehlgeschlagen. USB-Stick nicht optimal und Tutorial veraltet.

Neuen USB-Stick gekauft mit mehr Leistung neue Herangehensweise gefunden.

Quelle: [(51) [2021] KALI PERSISTENT auf USB installieren - YouTube](https://www.youtube.com/watch?v=ycnC1j9usTM&t=77s&ab_channel=TheMorpheusTutorials)





Leider Fehlermeldung. Nach langem recherchieren herausgefunden, das Secure Boot ausgeschalten werden muss. 

# Terminal Übungen

Quelle: <https://youtube.com/playlist?list=PLNmsVeXQZj7oaopPUB0SEmzZLf3aE5msy> Playlist bis Video 12 geschaut.

Apt-get update = Sucht nach verfügbare Updates

Apt-get upgrade = ladent die updates herunter

Apt-get dist-upgrade = neuste version von linux herunterladen

Root = man hat alle rechte. Da hinter Nutzer.

Pwd = Man sieht wo man sich momentan befindet

Ausgeschrieben «Print working directory»

Ls = Man sieht alles wo sich im momentanen Spacefolder befindet Ausgeschrieben «List»

Cd = change directory, so kommt man in neue Verzeichnise hinein

Touch = erstellen einer datei

Cp = kopiert eine datei in ein verzeichnis

Rm -r = Löschen einer datei ausgeschrieben «remove rekursiv» löscht ordner inklusiv seiner dateien oder kann auch einzelne dateien löschen

Rmdir = löscht ordner

Mkdir = make directory = erstellt ordner

Mv = move man kann es nutzen um eine Datei in eine neue zu transformieren, oder zb move file file1| hiermit wird file gelöscht und file 1 wird erstellt mit den gleichen inhalt wie file.  
Oder man kann es in ein Verzeichnis verschieben mv file ordner/»Name des files in dem ordner»

Nun wird das file in den ordner verschoben mit dem neuen namen

Cat = kann inhalt einer oder mehreren dateien ausgeben oder kann auch texte zusammenfügen. Steht für «concatenate»

Echo = mit diesem befehl kann man text in eine datei einfügen. > = inhalt wird überschrieben.  
>> text wird hinzugefügt.

-o = output es generiert den output wo man es will zbs

--help = zeigt alle mögliche befehle an

Ls -l = somit sieht man wer welche rechte hat

Ls -la = man sieht welche rechte jeder bei allem hat

111 = alle rechte = 7

101 = lese und ausführechte =5

100 = leserechte aber keine schreib und ausführechte. =4

Befehl chmod = rechte verteilen

./ = zum ausführen einer datei (geht nur bei ausführbaren dateien

Ps = zeigt laufende prozesse und mit -e zeigt every prozess an mit -ef zeigt es full format an = alle informationen

Kill = einen prozess beenden

Apt-get install wmctrl && wmctrl -l = gibt eine Liste von allen offenen fenstern

Apt-get install xdotool && xdotool search –name “namevomprogramm siehe wmctrl list” windowkill = schliesst ein programm

Crunch = erzeugt wörterlisten mit möglichen combinationen zbs für passwörter. Der befehl sieht ungefähr so aus

Crunch <min> <max> [welche zeichen] [optionen]

Reboot = neustarten des systems

Service «gewünschter service» restart = einen service wieder starten

Jobs = man zeigt die laufenden jobs an

Fg «idjob» = bringt den Job in der vordergrund

Bg «Idjob» = bringt den job in den hintergrund

Head -nx = gibt x viele zeilen von oben aus

Tail -nx = gibt x viele zeilenyl von unten betrachtet aus

Grep = mit diesem befehl kann man daten in einem file suchen zbs. Grep passwort file

Dieser befehl gibt alle zeilen aus welche das wort passwort beinhalten im file file

Grep -i = ignoriert lower-upper case

Grep -n = gibt noch die zeile aus

Grep -r = gibt ganzes verzeichnis aus

Grep -E = flexibleres suchen beispiel grep -E passwor[dt] sucht nach beiden schreibweisen

Grep -E [0-9] file sucht nach zahlen

Grep -E «rt|rd» sucht alles wo rt oder rd beinhaltet.

Grep -E «passwor[dt][^l] = sucht password/t aber nach dem darf kein l kommen

Grep -E passwor[dt]\1 = man bekommt das passwort 1

Grep -E s+ file = gibt alles mit mindestem einem s raus

Grep -E s\*wo = gibt alles an wo 0-x s hat in Verbindung mit dem Wort danach

Grep -E s?wo = eins oder keins

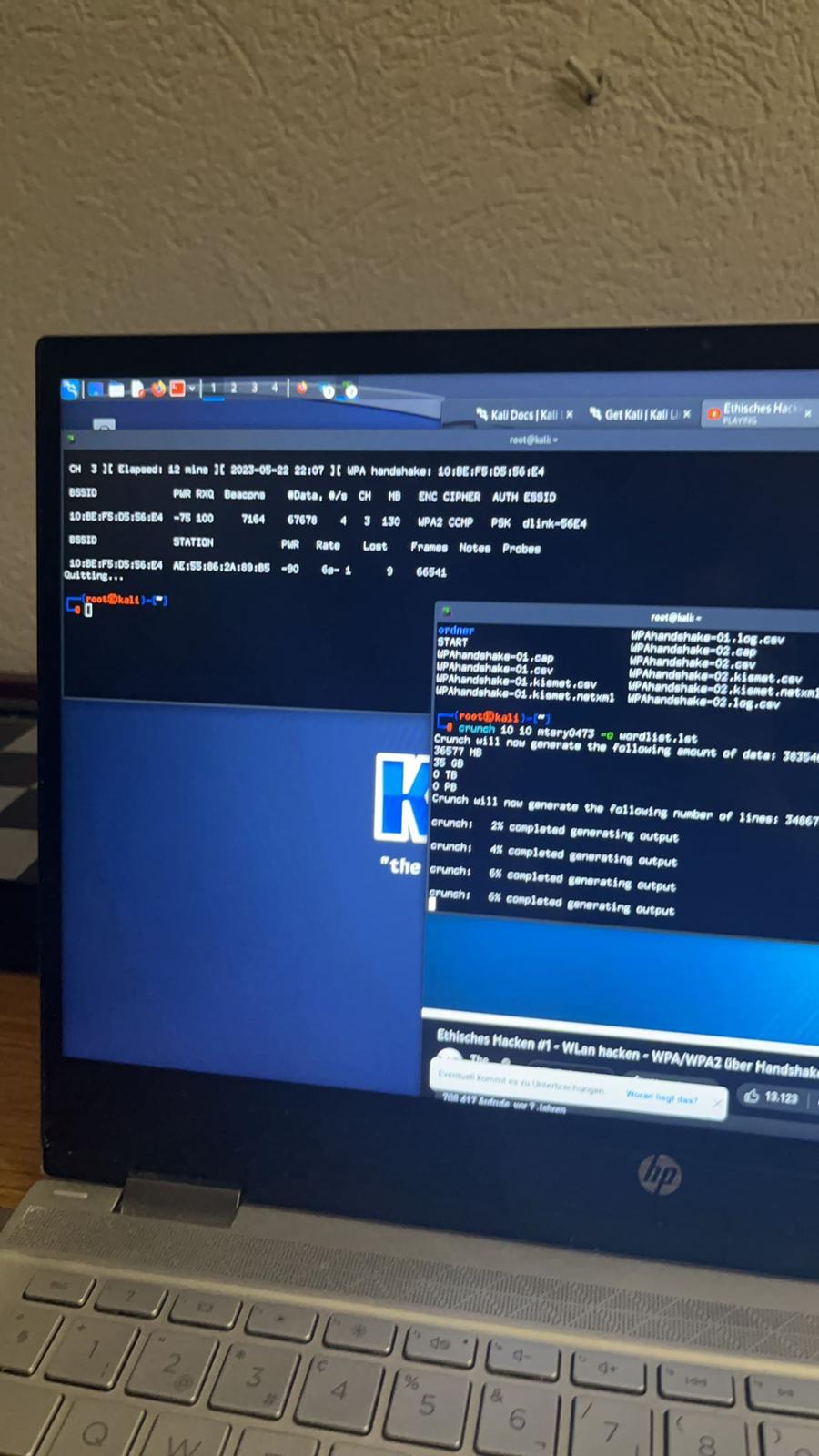
Grep -E s{2}wo = gibt alles an was 2 ss wo hat.

Mit -w kann man machen das nur ganze Wörter herauskommen

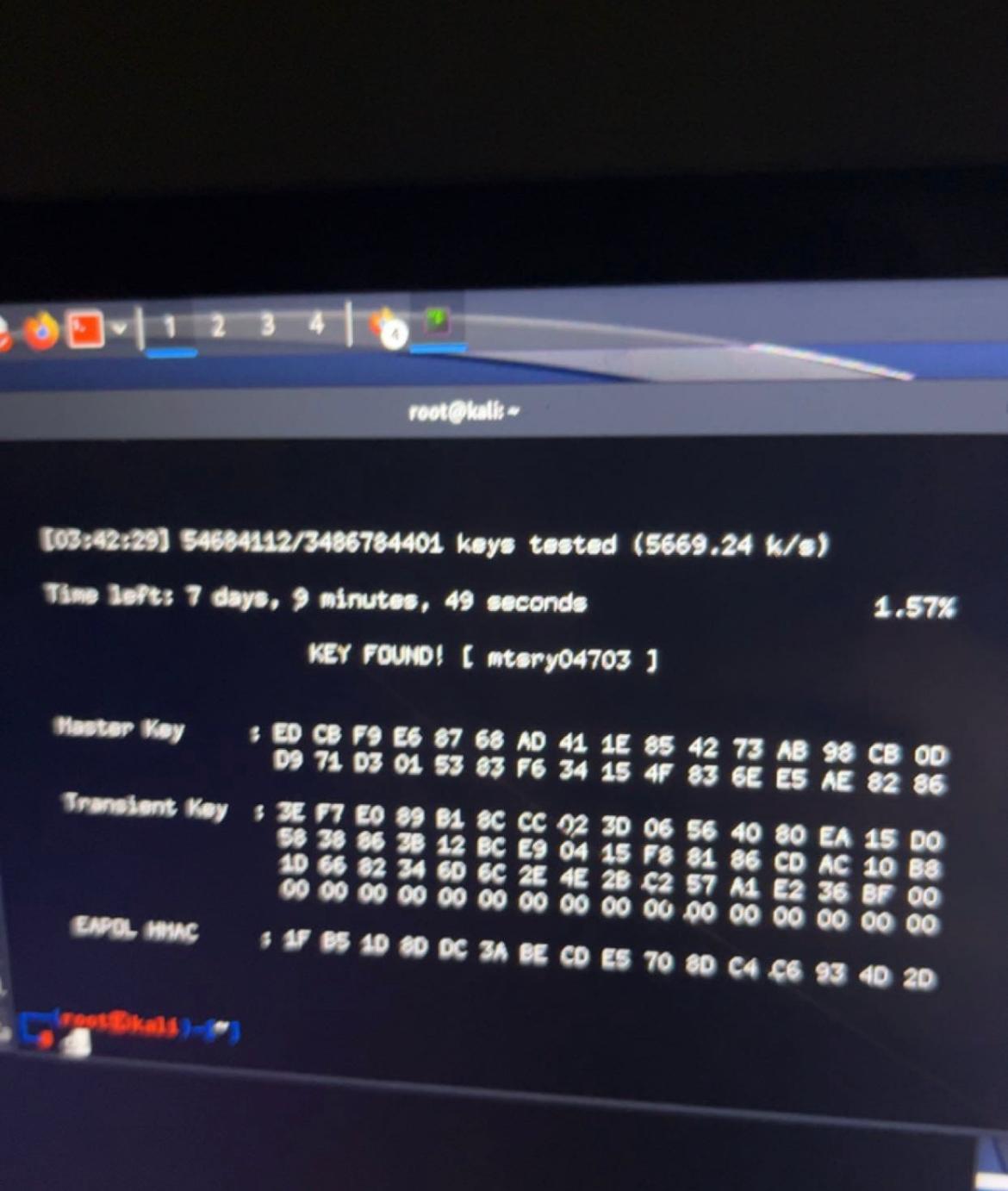
Es gibt noch viele weitere Möglichkeiten.

# Wlan Passwort knacken

Quelle: [(51) Ethisches Hacken #1 - WLan hacken - WPA/WPA2 über Handshake - Bruteforce - YouTube](https://www.youtube.com/watch?v=GLmpLeghM2Y&list=PLNmsVeXQZj7r3cONM-b6UgiW7Bu3LgMd-&ab_channel=TheMorpheusTutorials)

Genau wie im Video vorgegangen.  


Handshacke abgefangen und Crunch Liste erstellt.



Brute Force beendet nach 4h.