Project Name: Secure Kali Drive

Date: March 30, 2024

Created and performed by: Jason Patrick Salerno

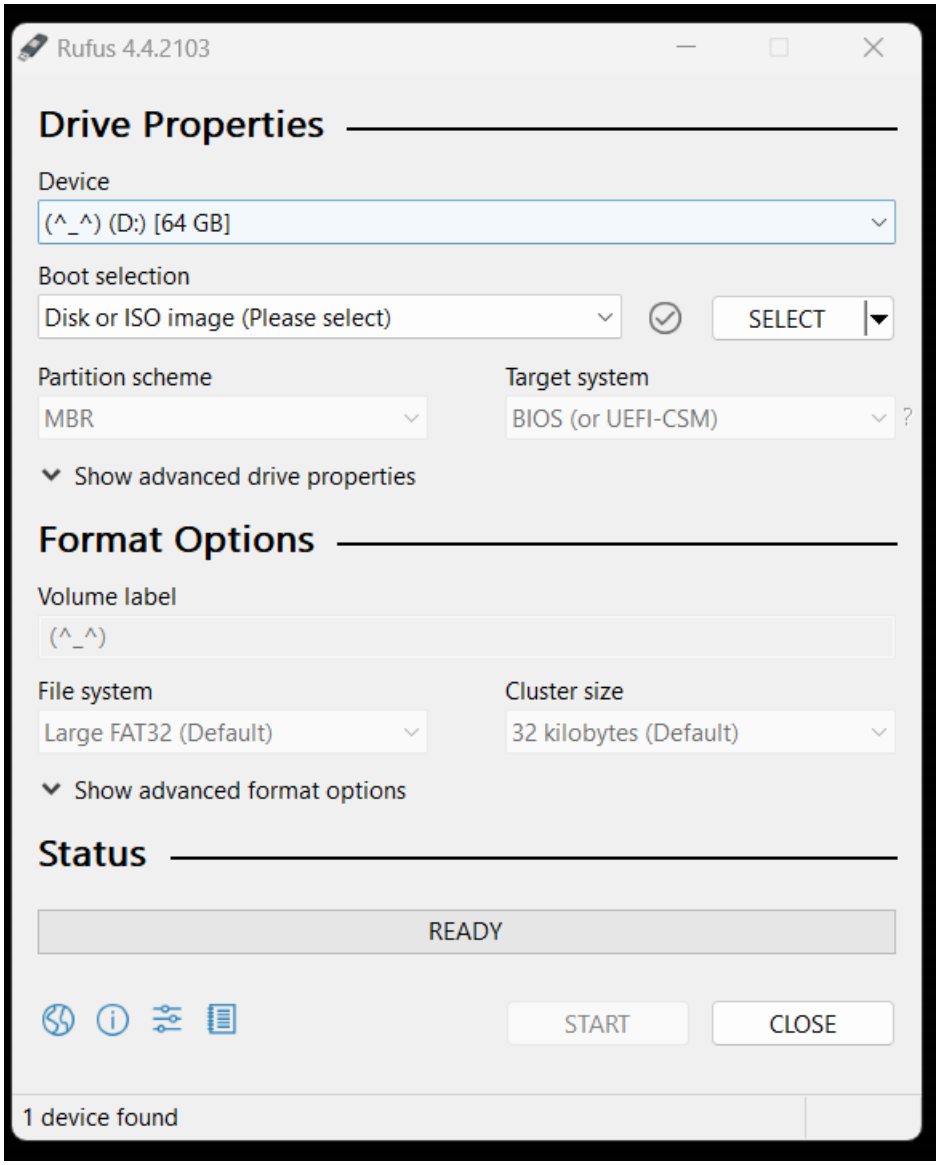
Purpose: To help cybersecurity students with their first secure live OS on a flash drive.

Part 1 Loading the kali Linux .iso image file onto the flash drive.

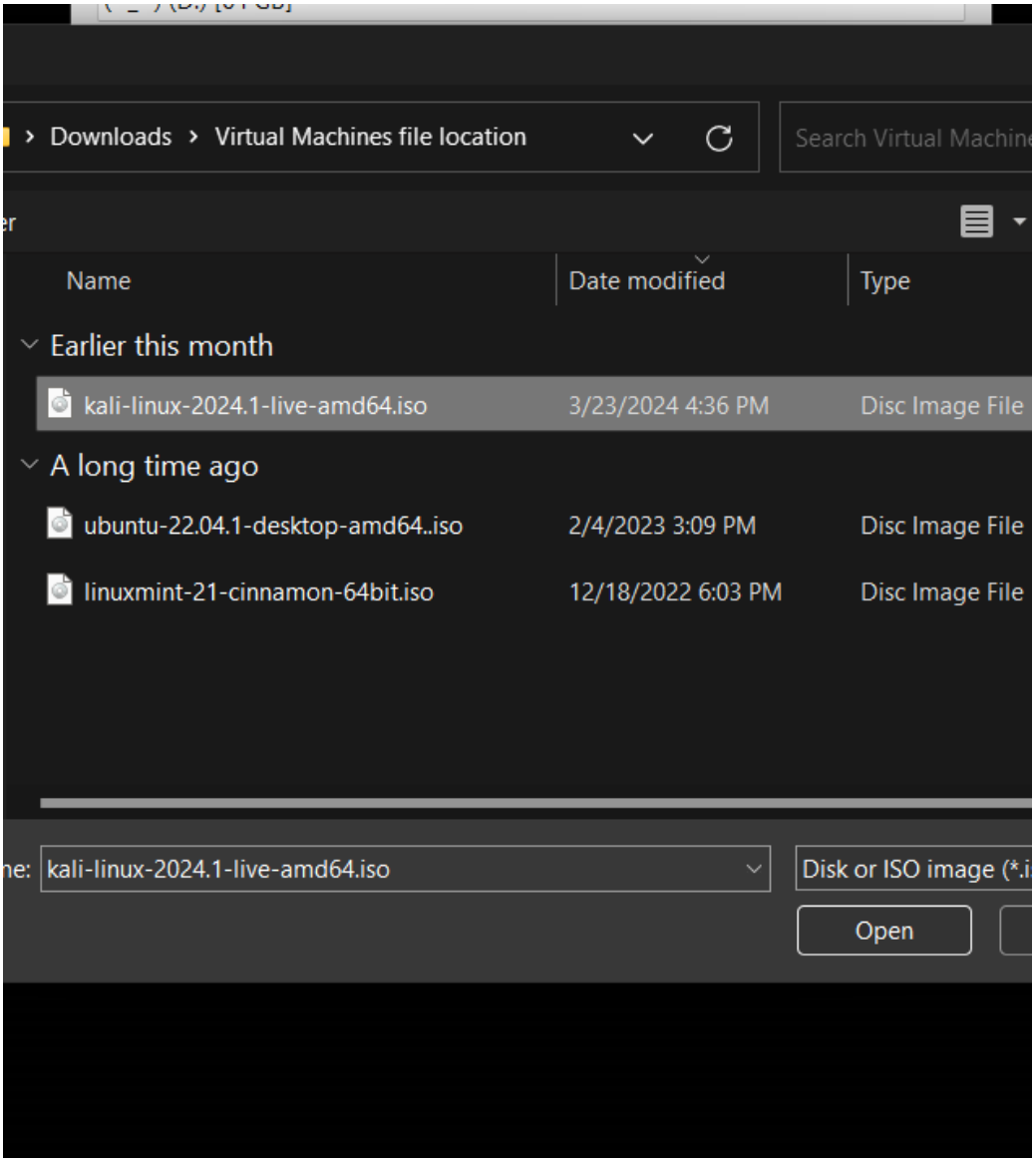
1. Find a flash drive you want to use for the kali Linux as a live bootable system with encrypted persistence.

2. Assuming you have already installed rufus, plug in the flash drive onto your machine and rufus will automatically detect the flash drive.

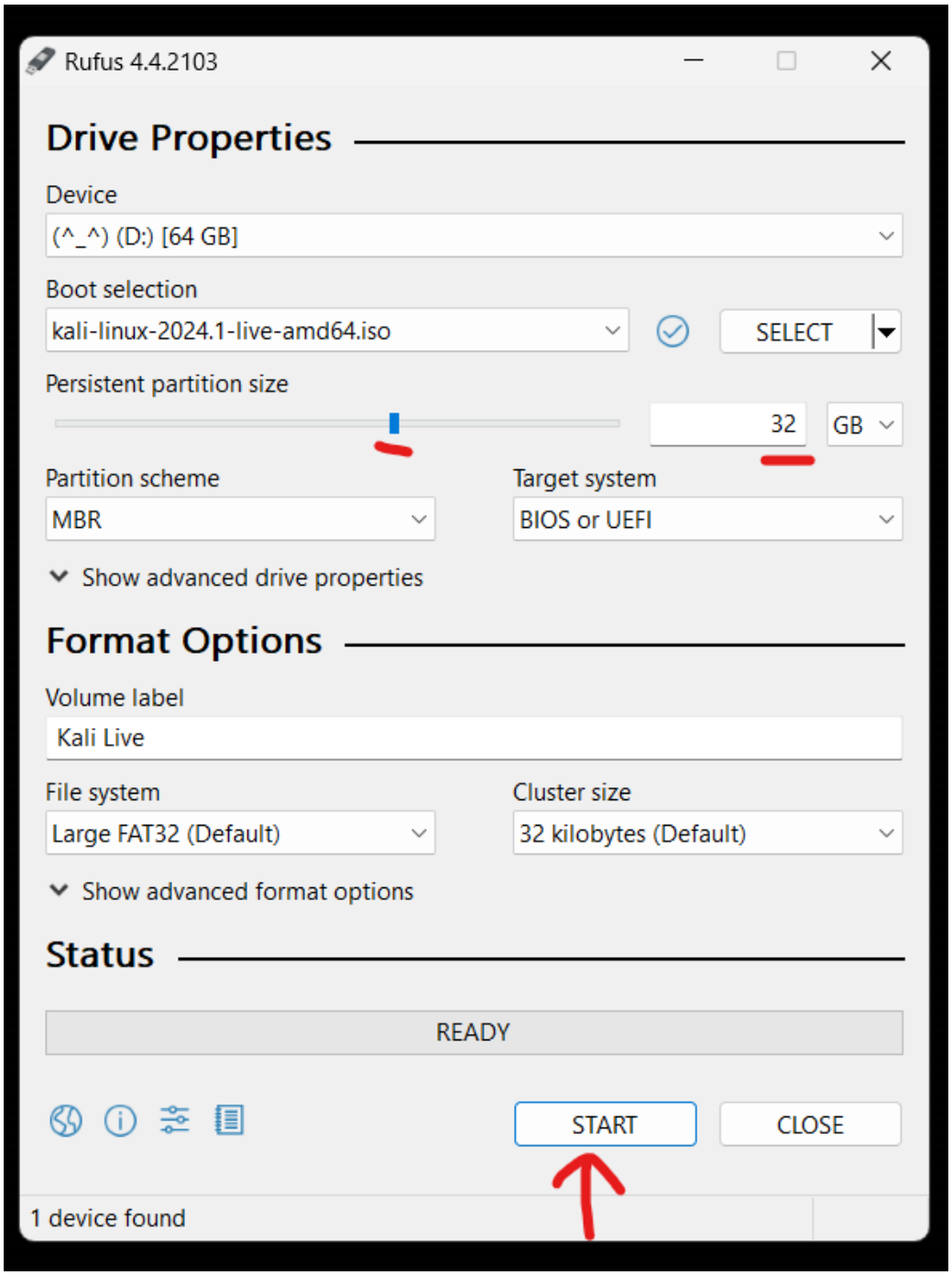
   Note: you have not installed rufus, yet you can download rufus here.



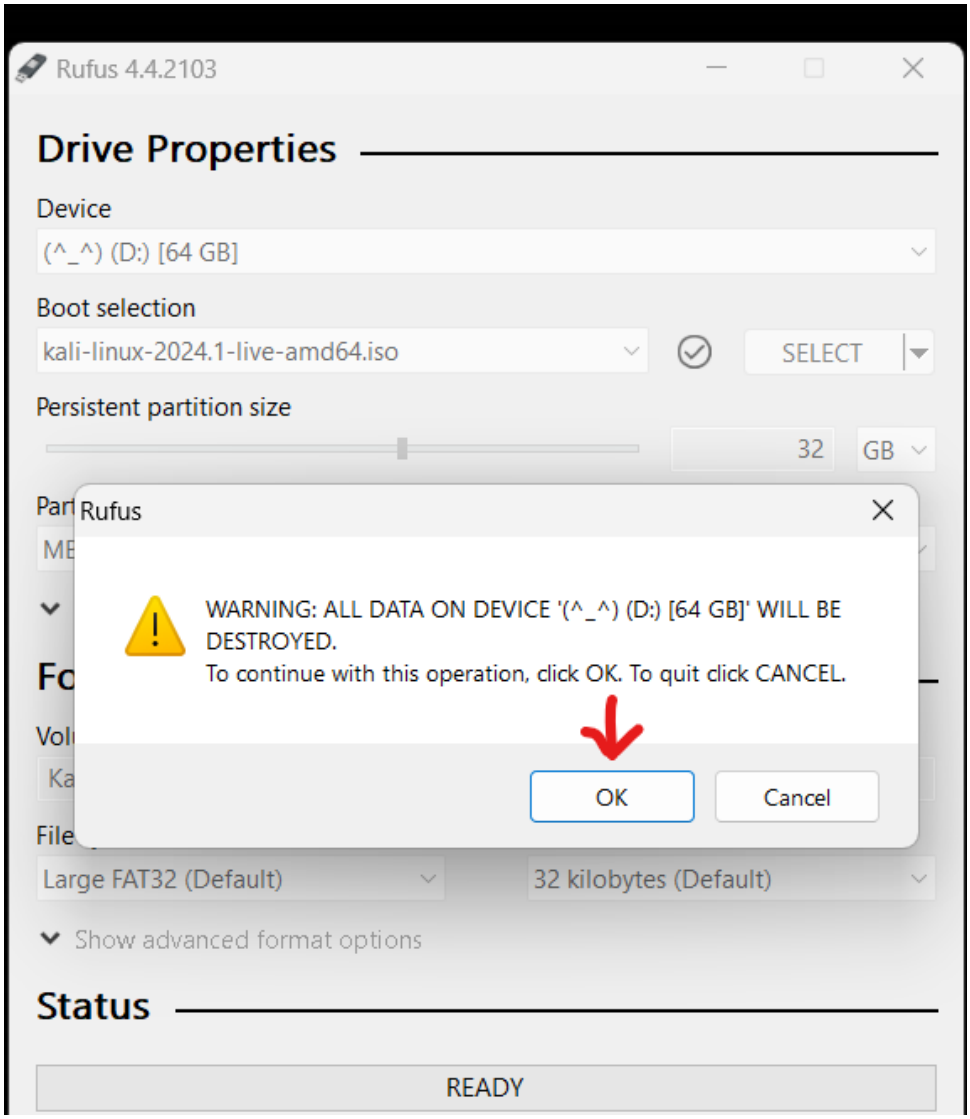
3. Next locate your kali Linux .iso image file and click on open.



4. Next set the desired amount of GB or space for the persistent partition on the flash drive.

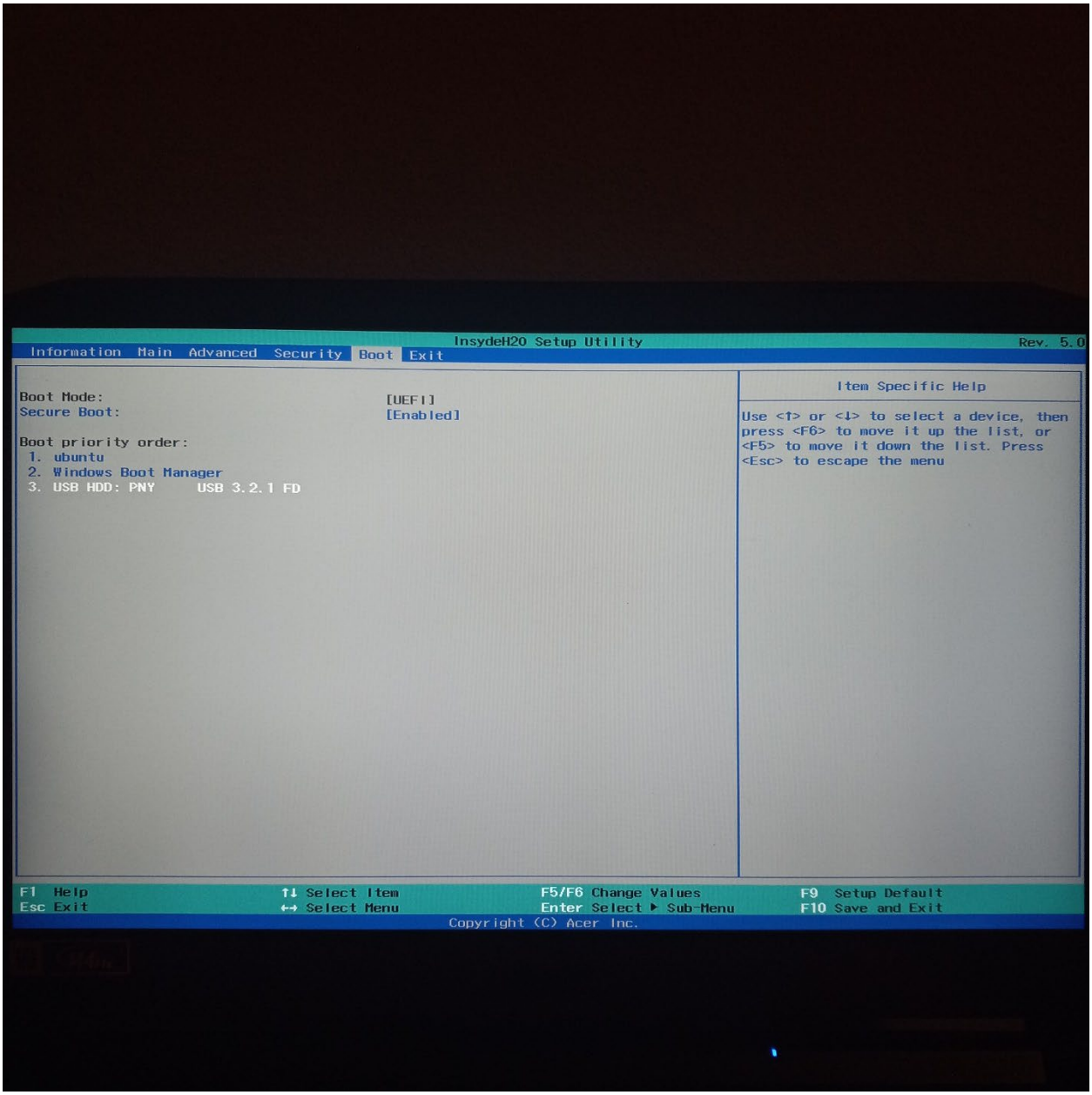


1. After clicking start, a warning will be displayed indicating that all data on the flash drive will be deleted. Click on OK. This will start formatting the flash drive by using the kali Linux image (.iso file).

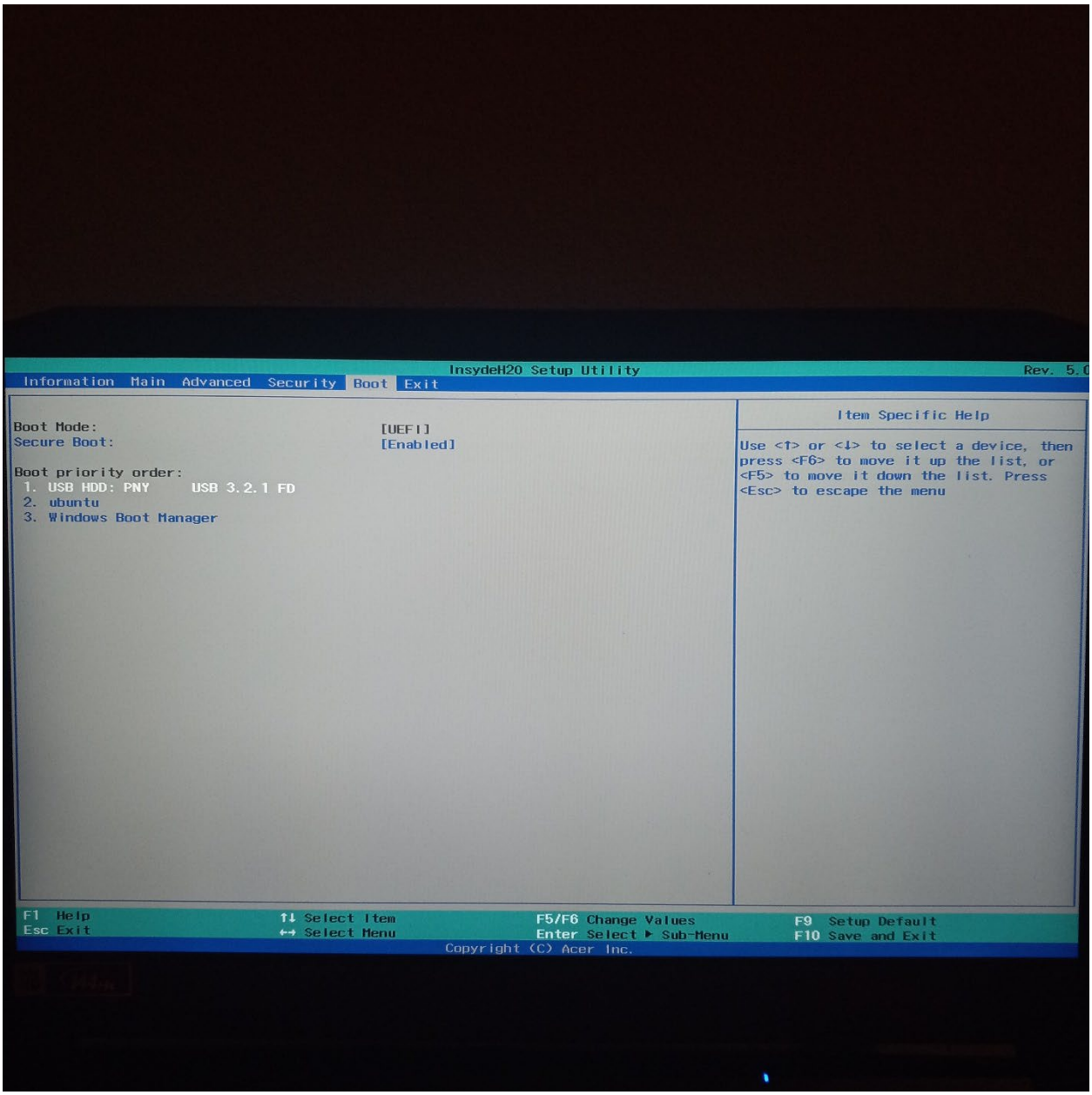


Part 2 Changing BIOS boot order & CLI configurations

1. Next do the following: Power on device > Press F2 consistently > Navigate to boot order > Press F6 to move up flash drive to make it the first boot order.



2. After you have changed the boot order to your flash drive navigate to exit and save changes. This will cause the machine to boot from the flash drive since you have changed the boot order.



3. After booting into kali Linux, navigate to the terminal and run the command below and look for your flash drive or logical partition on the flash drive**.** The fdisk -l command will list all the current partitions on the flash drive and your machine's current partition.

   Command: fdisk –l

   Note: Make sure you have root privileges to run this command. Output omitted.

   The highlighted section is the partition that I will be working on, yours may vary.

```
┌──(root㉿kali)-[~]
└─# fdisk -l
Disk /dev/nvme0n1: 931.51 GiB, 1000204886016 bytes, 1953525168 sectors
Disk model: Samsung SSD 980 PRO 1TB
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 4DA8BA8A-A771-465E-AD12-D1F4B81BCCB7









Partition table entries are not in disk order.


Disk /dev/sda: 57.77 GiB, 62026416128 bytes, 121145344 sectors
Disk model: USB 3.2.1 FD
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x030b86c6

Device     Boot    Start       End  Sectors  Size Id Type
/dev/sda1  *        2048  54036415 54034368 25.8G  c W95 FAT32 (LBA)
/dev/sda2       54036416 121145275 67108860   32G 83 Linux
```

4. After locating the desired partition to use, execute the command below.

   Command: cryptsetup –verbose –verify-passphrase luksFormat /dev/sda2.
   Note: this command requires root privileges.

```
Disk /dev/sda: 57.77 GiB, 62026416128 bytes, 121145344 sectors
Disk model: USB 3.2.1 FD
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x030b86c6

Device     Boot    Start       End  Sectors  Size Id Type
/dev/sda1  *        2048  54036415 54034368 25.8G  c W95 FAT32 (LBA)
/dev/sda2       54036416 121145275 67108860   32G 83 Linux


Disk /dev/loop0: 3.49 GiB, 3748089856 bytes, 7320488 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

┌──(root㉿kali)-[~]
└─# cryptsetup --verbose --verify-passphrase luksFormat /dev/sda2
WARNING: Device /dev/sda2 already contains a 'ext3' superblock signature.

WARNING!
========
This will overwrite data on /dev/sda2 irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /dev/sda2:
Verify passphrase:
Existing 'ext3' superblock signature on device /dev/sda2 will be wiped.
Key slot 0 created.
Command successful.

┌──(root㉿kali)-[~]
└─# cryptsetup luksOpen /dev/sda2 cyber_sec
Enter passphrase for /dev/sda2:
```

5. After executing the command, you need to add a passphrase. This will protect your secure kali drive from unauthorized access. Make sure to have at least a 10-15 character passphrase for enhance security.

   Note: Linux commands are case-sensitive.
   Command: cryptsetup –verbose –verify-passphrase luksFormat /dev/sda2

```
┌──(root㉿kali)-[~]
└─# cryptsetup --verbose --verify-passphrase luksFormat /dev/sda2
WARNING: Device /dev/sda2 already contains a 'ext3' superblock signature.

WARNING!
========
This will overwrite data on /dev/sda2 irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /dev/sda2:
Verify passphrase:
Existing 'ext3' superblock signature on device /dev/sda2 will be wiped.
Key slot 0 created.
Command successful.

┌──(root㉿kali)-[~]
└─# cryptsetup luksOpen /dev/sda2 cyber_sec
Enter passphrase for /dev/sda2:

┌──(root㉿kali)-[~]
└─# mkfs.ext3 /dev/mapper/cyber_sec
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 8384511 4k blocks and 2097152 inodes
Filesystem UUID: e58cf055-d2d4-4633-8997-854531122767
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Allocating group tables: done
Writing inode tables: 76/256
```

6. Next open the Linux Unified Key Setup (LUKS setup) , then create an ext3 filesystem to your specified directory.

   Command: cryptsetup luksOpen /dev/your_flash_drive_partition
   Command: mkfs.ext3 /dev/mapper/your_created_parition_name.

```
┌──(root㉿kali)-[~]
└─# cryptsetup luksOpen /dev/sda2 cyber_sec
Enter passphrase for /dev/sda2:

┌──(root㉿kali)-[~]
└─# mkfs.ext3 /dev/mapper/cyber_sec
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 8384511 4k blocks and 2097152 inodes
Filesystem UUID: e58cf055-d2d4-4633-8997-854531122767
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks):
done
Writing superblocks and filesystem accounting information:
done


┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#
```

7. Add a label to your ext3 file system and specify your flash drive's partition or your flash drive's directory in general.

   Command: e2label /dev/mapper/your_flash_drive_partition desired_label.

```
┌──(root㉿kali)-[~]
└─# mkfs.ext3 /dev/mapper/cyber_sec
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 8384511 4k blocks and 2097152 inodes
Filesystem UUID: e58cf055-d2d4-4633-8997-854531122767
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks):
done
Writing superblocks and filesystem accounting information:
done


┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# e2label /dev/mapper/cyber_sec persistence
```

8. After adding a label to your flash drive's partition, it's time to create a directory inside the /mnt (mount) directory. The `-p` option helps create nested directories smoothly without causing errors if they already exist.

   Command: mkfs.ext3 /dev/mapper/your_partition_name.

```
┌──(root㉿kali)-[~]
└─# mkfs.ext3 /dev/mapper/cyber_sec
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 8384511 4k blocks and 2097152 inodes
Filesystem UUID: e58cf055-d2d4-4633-8997-854531122767
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks):
done
Writing superblocks and filesystem accounting information:
done


┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# e2label /dev/mapper/cyber_sec persistence

┌──(root㉿kali)-[~]
└─# mkdir -p /mnt/cyber_sec
```

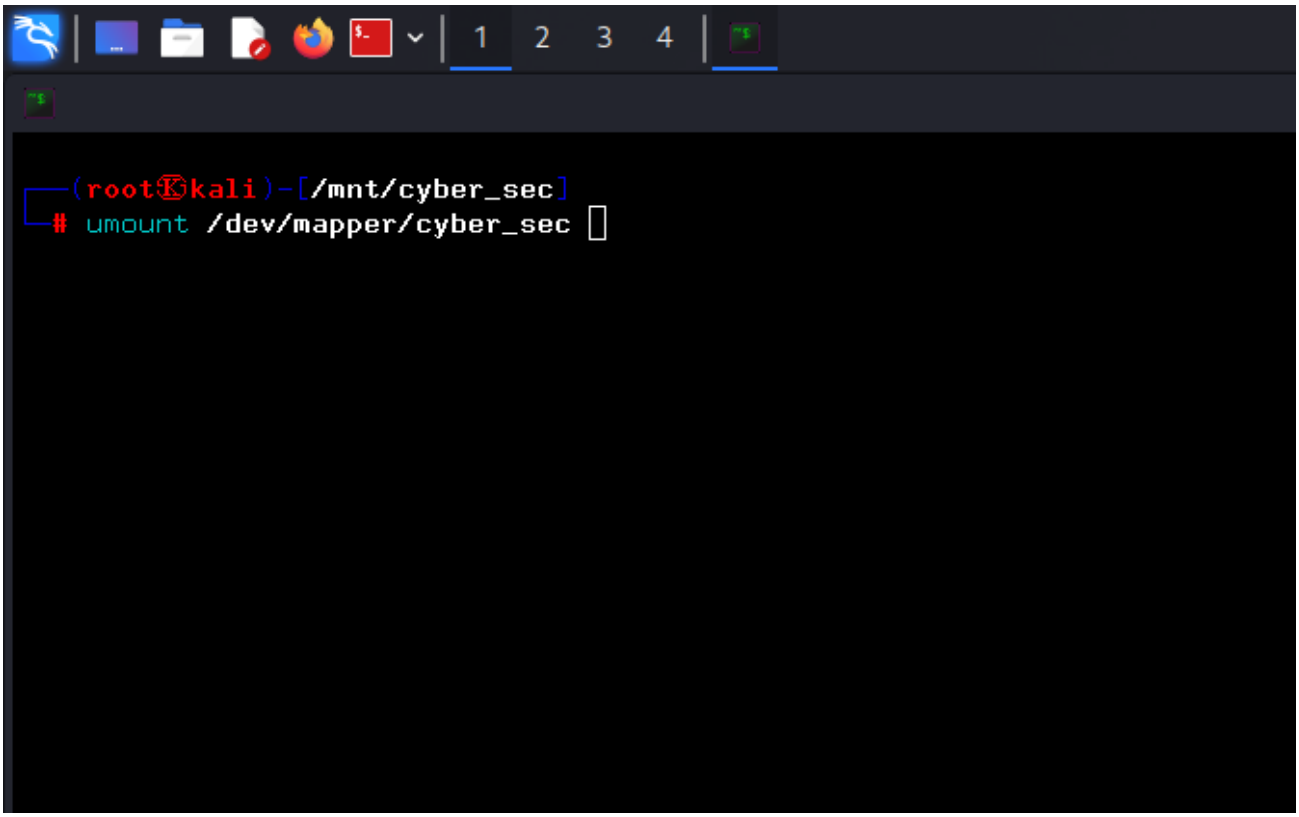
9. Next mount a filesystem that has been encrypted using LUKS onto a mount point in the Linux file system. Then change directory using the cd command with the specified directory and create a configuration file.

   Command: mount /dev/mapper/your_fd_partition /mnt/your_fd_partition.
   cd /mnt/your_fd_partition
   touch persistence.conf

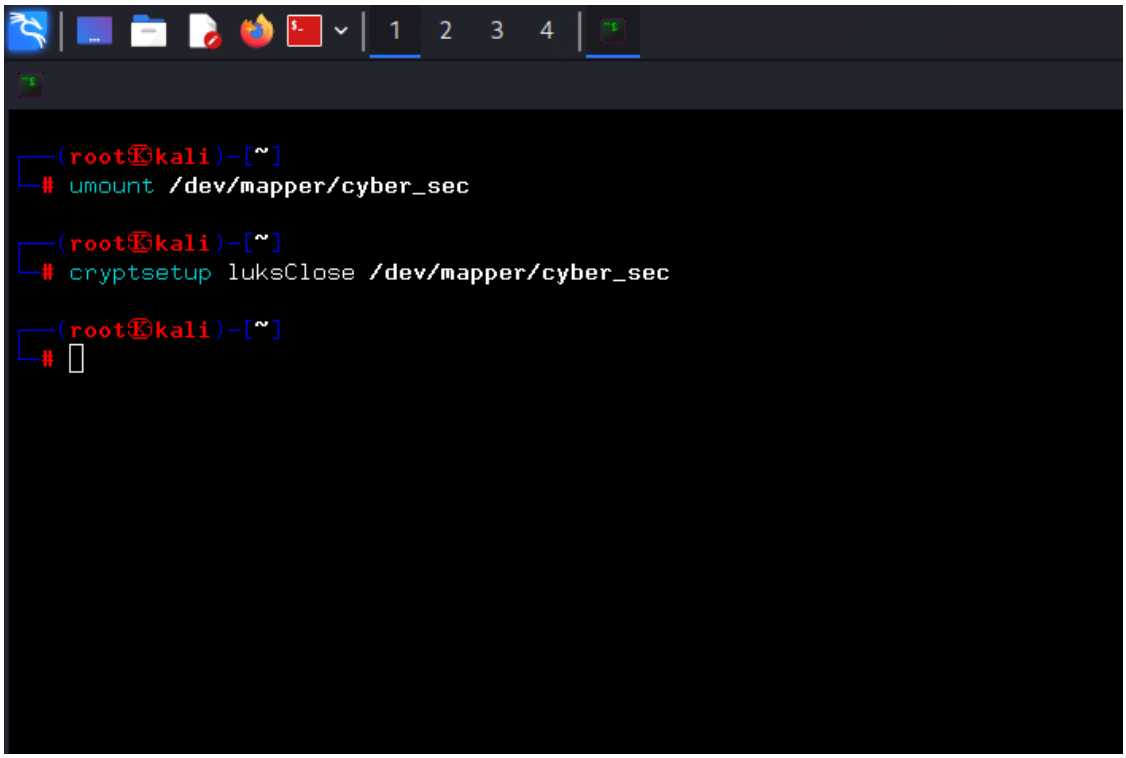
   Note: use nano or vim to add the '/union' text onto the configuration file.

```
┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# e2label /dev/mapper/cyber_sec persistence

┌──(root㉿kali)-[~]
└─# mkdir -p /mnt/cyber_sec

┌──(root㉿kali)-[~]
└─# mount /dev/mapper/cyber_sec /mnt/cyber_sec

┌──(root㉿kali)-[~]
└─# cd /mnt/cyber_sec

┌──(root㉿kali)-[/mnt/cyber_sec]
└─# touch persistence.conf
```

10. Then unmount your flash drive's partition or your flash drive in general.
    Command: umount /dev/mapper/your_fd_partition.



11. And finally, close the LUKS setup on the flash drive.
    Command: cryptsetup luksClose /dev/mapper/your_flash_drive.



References

Download Kali Linux Image file (.iso): https://www.kali.org/get-kali/#kali-live

Download Rufus for loading a .iso file onto a flash drive: https://rufus.ie/en/

Kali Linux Encrypted Persistence CLI configuration: https://youtu.be/A1ZxEJHUIUU

Note: Only use this tool for ethical purposes. Also make sure to check the md5 hash value or SHA1 hash value before and after downloading the kali Linux image file (.iso), to make sure the .iso image you downloaded has not been tampered with.

By: JPS

End of Documentation