

Case Name: The Imaging Process

Couse Name: IST402

Instructor: Robert Price

Date: 02/03/2025

Examiner Name: Jaspreet Singh

Table of Contents

LIST OF ILLUSTRATIVE MATERIALS	3
TABLES	3
FIGURES	3
EXECUTIVE SUMMARY	4
BACKGROUND	4
EVIDENCE	4
COLLECTION AND ANALYSIS	4
COLLECTION	5
ANALYSIS	5
FTK Imager	5
dd	10
Kali	11
CONCLUSION	12
FTK imager	12
dd	13
Kali	13

List of Illustrative Materials

Tables	1
Table 1: Evidence	4
 Figures	5
FTK IMAGER	
Figure 1: Downloading FTK Application and Creating Image	5
Figure 2: Inputting Information for Image Creation	6
Figure 3: Saving Image under Backups	6
Figure 4: Verifying Correct Imaging	7
Figure 5: Verifying Hash Values	7
Figure 6: Seeing File Created	8
Figure 7: Verification Data	9
dd	
Figure 8: dd Partitioning.....	10
Figure 9: image.dd file size.....	11
Kali	
Figure 10: Kali disk and partitions	11
Figure 11: New Directory	12

EXECUTIVE SUMMARY

Background

Forensic imaging is the bit-by-bit process of copying storage media to ensure that digital evidence is preserved and unaltered. Simply powering on a system can affect files on that system, hashing techniques such as MD5 and SHA-1 ensure that the data copied is identical to the original data. Imaging can be either physical, which captures all data, including deleted files, or logical, which copies only selected files or partitions. Depending on whether the system is running, it can also be executed as a live or static acquisition. Various tools used for forensic imaging include FTK Imager-based GUI and Linux command-line-based dd/dcfldd, among others, with hashing to ensure integrity. In this report, the examiner will cover multiple imaging techniques and the importance of forensic integrity in investigations.

Evidence

Description	Hash Algorithm	Hash Value	Examiner
Evidence	MD5	487ffbf1657de0c11235daf2c91ef952	Jaspreet Singh
Evidence	SHA-1	B6a42d46c9089dc0797b9a42c80cff72aa1fd1c	Jaspreet Singh

COLLECTION AND ANALYSIS

Collection

Through this process the examiner was able to image and copy the original drive so that it can be used as evidence for analysis. This way of copying the original drive ensures that the data's integrity that is copied is secure and reliable to use for evidence. The examiner used Windows applications and tools such as AccessData FTK Imager 3.1.3.2, command prompt, dd, and kali to help create the forensic images needed for this analysis.

Analysis

Downloading the FTK Imager application

The examiner downloaded the AccessData FTK Imager 3.1.3.2 in Windows and will now begin creating a new disk image.

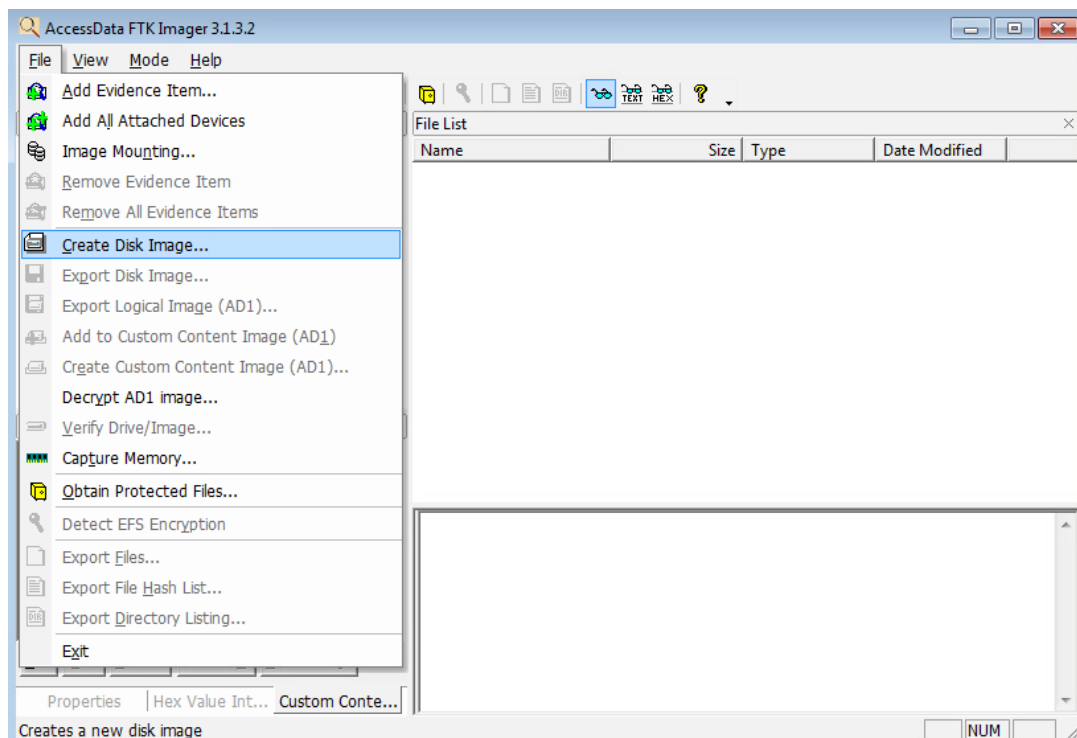
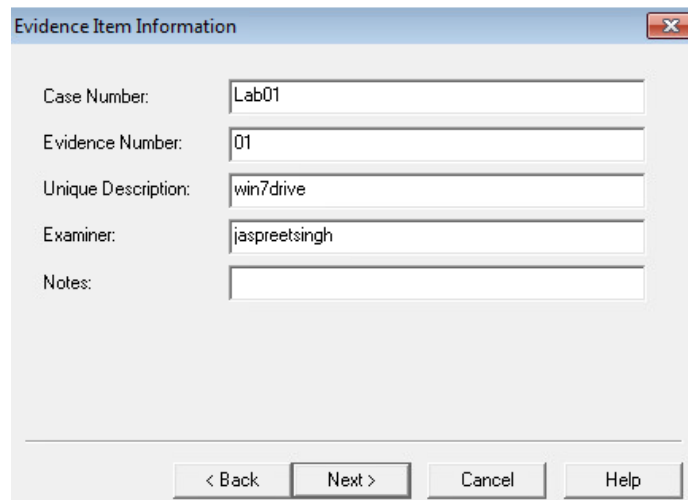


Figure 1: Downloading FTK Application and Creating Image

Inputting Information to Create Image

After creating a disk image, the examiner starts inputting the Evidence Item information to continue with the imaging process. The examiner inputted the information as shown below in screenshot.



Evidence Item Information	
Case Number:	Lab01
Evidence Number:	01
Unique Description:	win7drive
Examiner:	jaspreetsingh
Notes:	

< Back Next > Cancel Help

Figure 2: Inputting Information for Image Creation

Saving Image to destination Folder

The examiner has put the image filename as image.dd and the image has been fragmented to the size of zero. Now the examiner will save the image destination folder to the computers NTFS(H:) drive under Backups.

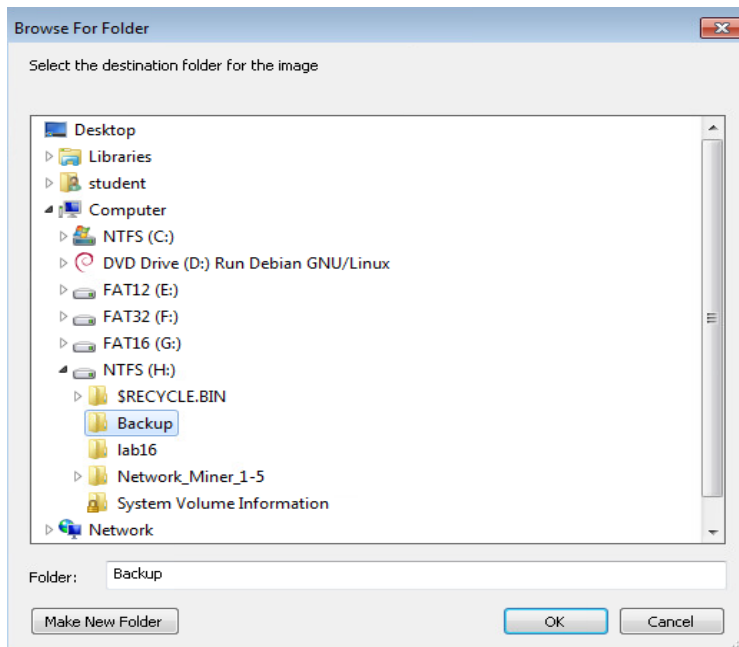


Figure 3: Saving Image under Backups

Verification of Copy Image

The examiner has finished saving and inputting information for the new forensic image and is now creating the image to get verification of the correct copy so that the examiner can begin analyzing the data.

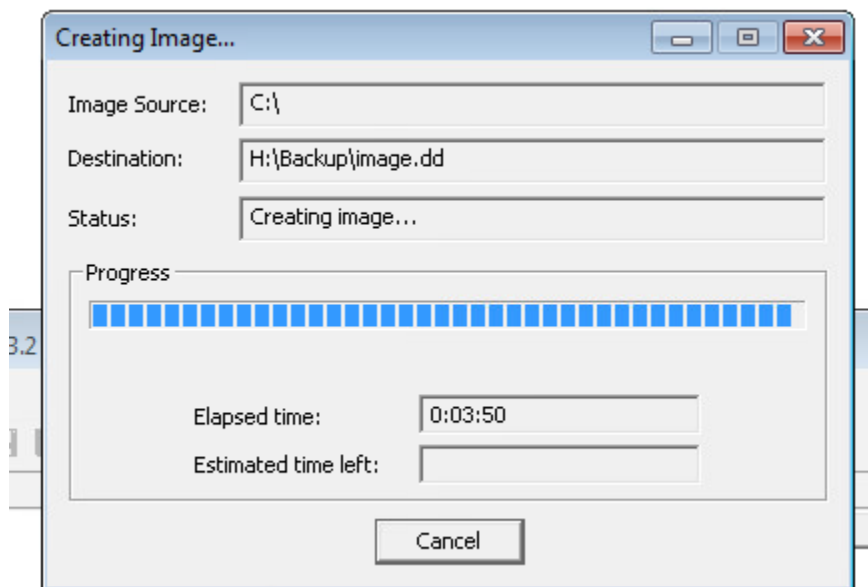


Figure 4: Verifying Correct Imaging

Hashing Created from Image MD5 and SHA1

The examiner has finished creating the image and has noted the hash values for MD5 and SHA1 by verifying they both match. Matching hashes verify that the digital image created is not different and the integrity of the data remains true.

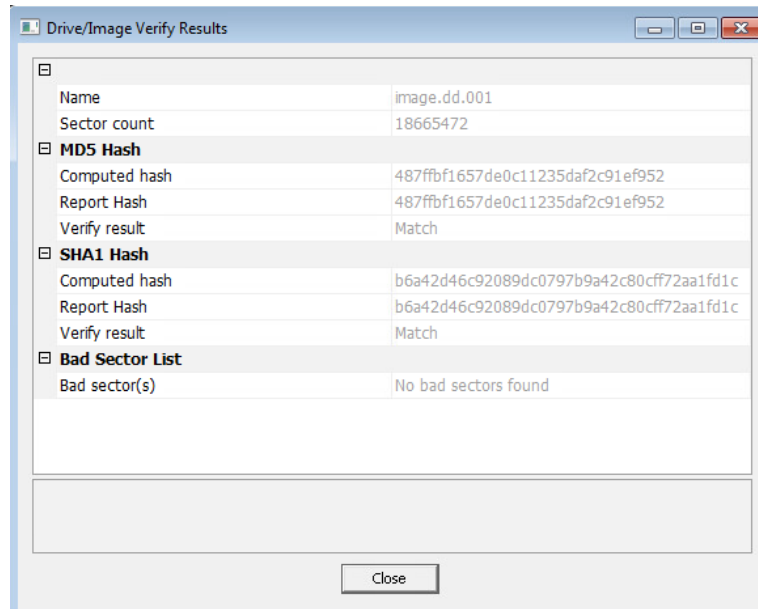


Figure 5: Verifying Hash Values

Copy File

The examiner, after verifying the hash values, can now look at the image.dd.001.txt file to verify correct copying. The examiner is able to look at the file and open it to see the information.

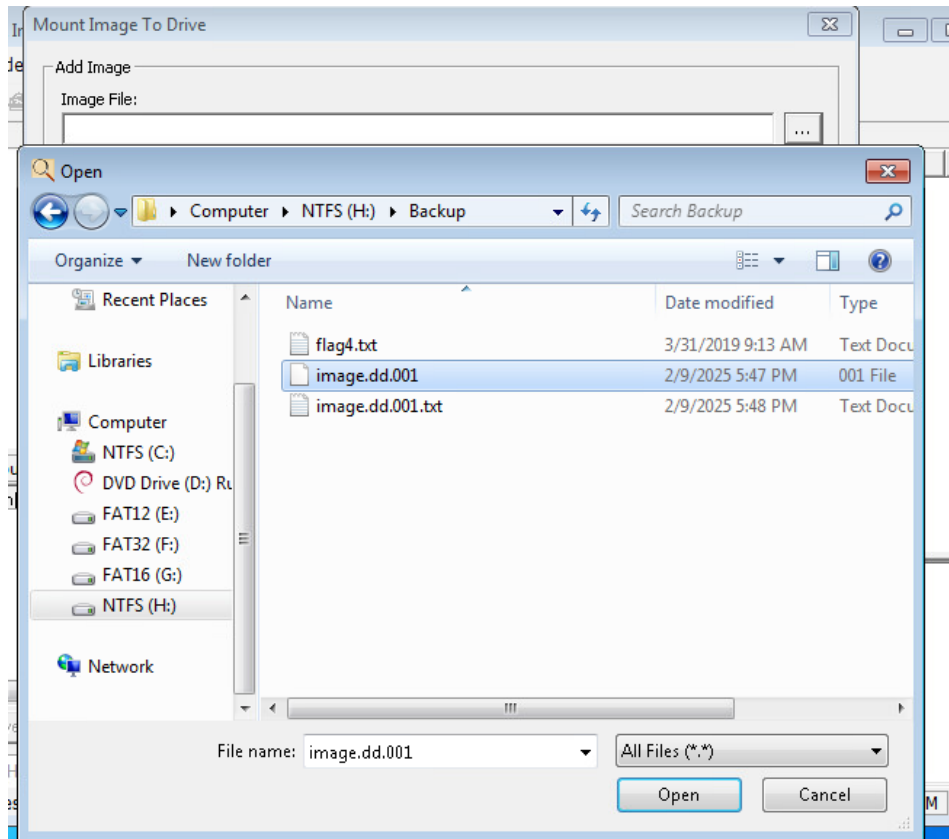


Figure 6: Seeing File Created

Verification Data Contents in File

The examiner has opened the image.dd.001 file and has gotten confirmation of the copying process. Confirmation is shown in the screenshot below showing that the MD5 and SHA1 hash values have been verified.

```
image.dd.001.txt - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 3.1.3.2

Case Information:
Acquired using: ADI3.1.3.2
Case Number: Lab05
Evidence Number: 01
Unique description: win7drive
Examiner: jaspreetsingh
Notes:

-----

Information for H:\Backup\image.dd:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 18,665,472
[Physical Drive Information]
Removable drive: False
Source data size: 9114 MB
Sector count: 18665472
[Computed Hashes]
MD5 checksum: 487ffbfb1657de0c11235daf2c91ef952
SHA1 checksum: b6a42d46c92089dc0797b9a42c80cff72aa1fd1c

Image Information:
Acquisition started: Sun Feb 09 17:43:20 2025
Acquisition finished: Sun Feb 09 17:47:15 2025
Segment list:
H:\Backup\image.dd.001

Image Verification Results:
Verification started: Sun Feb 09 17:47:15 2025
Verification finished: Sun Feb 09 17:48:31 2025
MD5 checksum: 487ffbfb1657de0c11235daf2c91ef952 : verified
SHA1 checksum: b6a42d46c92089dc0797b9a42c80cff72aa1fd1c : verified
```

Figure 7: Verification Data

Command Prompt Information Collecting

The examiner uses the command prompt to find information inside flag5.txt and sees the disk partitions. Then executes the following prompt to partition.

```
C:\>dd if=\\.\e: of="h:\image.dd" --progress bs=1024
rawwrite dd for windows version 0.3.
written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL. See copying.txt for details
7,340,032
7168+0 records in
7168+0 records out

C:\>
```

Figure 8: dd Partitioning

Adding Records into File

The examiner can see in the computers NTFS(H:) drive that the following image.dd drive size is now 7,168 KB like in previous screenshots when adding records into file.

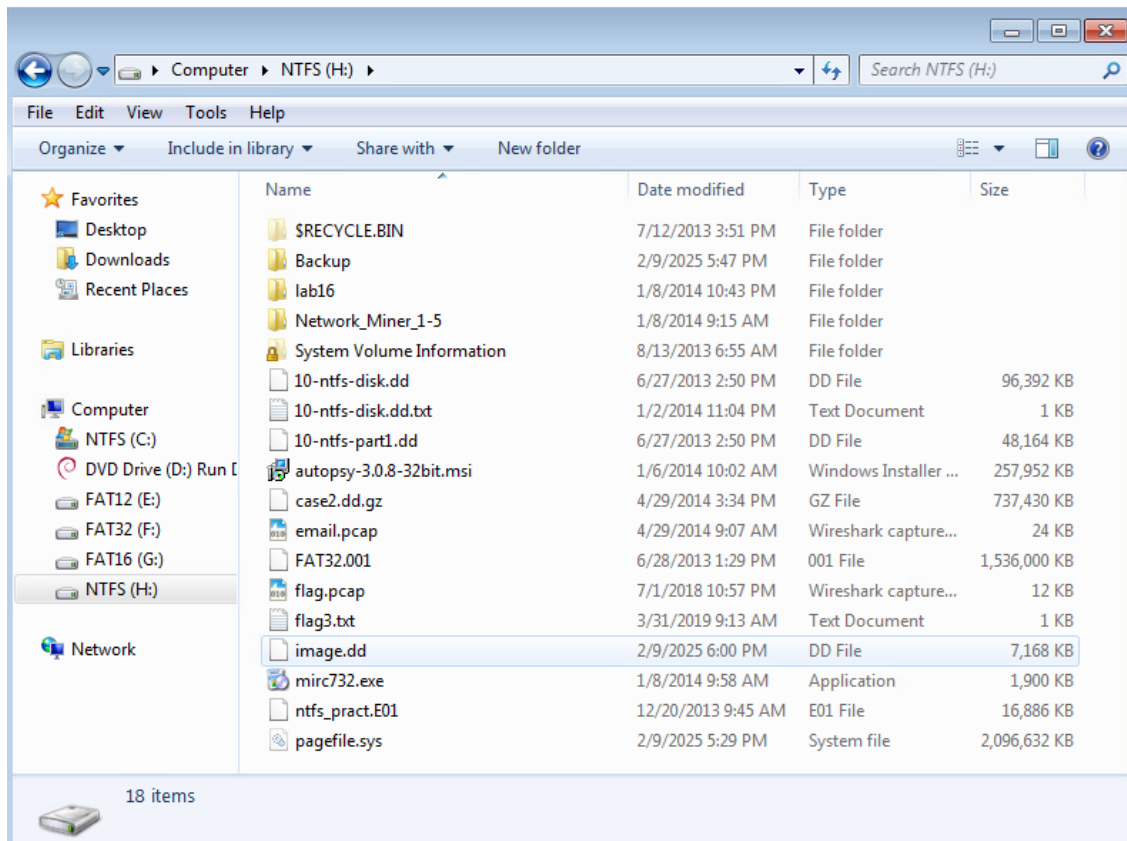


Figure 9: image.dd file size

Using Kali Terminal

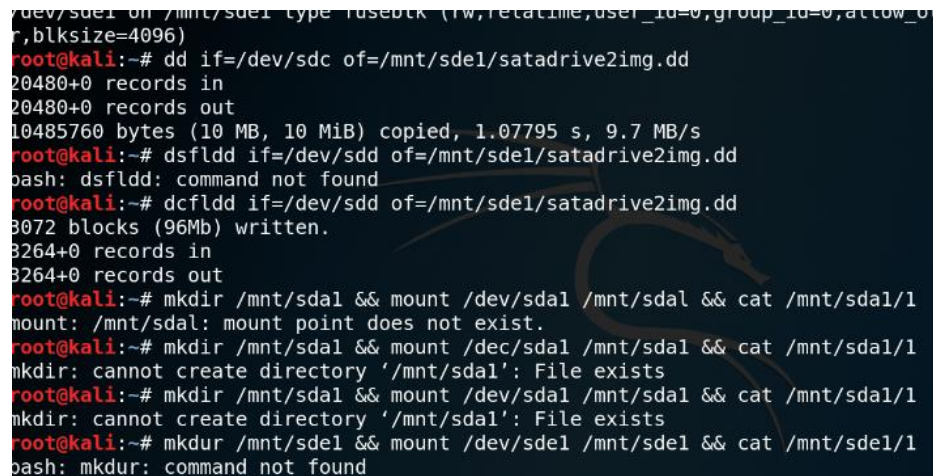
The examiner is now using Kali's terminal to display the disks and their corresponding partitions.

```
root@kali:~# mkdir /mnt/sdel
root@kali:~# ntfs-3g /dev/sdel /mnt/sdel
root@kali:~# mount | grep sde
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
/dev/sdel on /mnt/sdel type fuseblk (rw,relatime,user_id=0,group_id=0,allow_others,blksize=4096)
root@kali:~#
```

Figure 10: Kali disk and partitions

Creating Directory and Retrieving File

The examiner is creating a directory called sda4 and is mounting the partition from previous screenshot into the new directory.

A terminal window screenshot showing a series of commands and their outputs. The user is working in a Kali Linux environment. The commands include using 'dd' to copy data from /dev/sdc to a file, 'dsfdd' and 'dcfldd' for disk imaging, and several 'mkdir' and 'mount' attempts to create and mount a directory named /mnt/sdal. The outputs show the progress of data copying and the errors encountered when trying to create the directory and mount it.

```
dev/sde1 on /mnt/sde1 type fuseblk (rw,relatime,user_id=0,group_id=0,allow_ol
r,blksize=4096)
root@kali:~# dd if=/dev/sdc of=/mnt/sde1/satadrive2img.dd
20480+0 records in
20480+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 1.07795 s, 9.7 MB/s
root@kali:~# dsfdd if=/dev/sdd of=/mnt/sde1/satadrive2img.dd
bash: dsfdd: command not found
root@kali:~# dcfdd if=/dev/sdd of=/mnt/sde1/satadrive2img.dd
3072 blocks (96Mb) written.
3264+0 records in
3264+0 records out
root@kali:~# mkdir /mnt/sdal && mount /dev/sdal /mnt/sdal && cat /mnt/sdal/1
mount: /mnt/sdal: mount point does not exist.
root@kali:~# mkdir /mnt/sdal && mount /dev/sdal /mnt/sdal && cat /mnt/sdal/1
mkdir: cannot create directory '/mnt/sdal': File exists
root@kali:~# mkdir /mnt/sdal && mount /dev/sdal /mnt/sdal && cat /mnt/sdal/1
mkdir: cannot create directory '/mnt/sdal': File exists
root@kali:~# mkdun /mnt/sde1 && mount /dev/sde1 /mnt/sde1 && cat /mnt/sde1/1
bash: mkdun: command not found
```

Figure 11: New Directory

CONCLUSION

Conclusion

Overall, the examiner was able to use imaging techniques such as FTK imager, dd, and Kali to help create a duplicate copy of the original data as forensic evidence. This process ensures that the data being analyzed is not tampering with the original evidence and is reliable since hash values were matched during the copying process to ensure that integrity remains throughout the investigation.

FTK Imager

This is a GUI-based tool for forensic imaging that supports both physical and logical acquisitions with encryption options. It includes built-in hashing, a key advantage ensuring that the forensic image replicates the original. Hence, the data being analyzed in the duplicate file is reliable and safe. However, this FTK imager has one disadvantage on Windows: when files are locked in the operating system, it is less reliable when imaging.

dd

This command is a strong Linux tool for creating raw forensic images. It performs a bit-by-bit copy of the storage device, making it ideal for forensic investigations. dd is used on the command line, so it works faster than the FTK imager, but it requires more care and attention since command errors are easy to make.

Kali

Kali uses a command line prompt similar to dd and provides a much more controlled environment for copying files or data, specifically when booted from a Live CD, which would prevent systems from being modified.