**🧪 Experiment 2: Mirror Image Creation & Integrity Check using Kali Linux Forensic Tools**

**✅ Step-by-Step Procedure (from the PDF)**

**🔹 Step 1: Open Terminal**

bash

CopyEdit

# Open the terminal from your Kali Linux menu or use Ctrl+Alt+T

**🔹 Step 2: Attach the Source of Evidence**

* Insert the **Hard Disk / USB device / CD-ROM** you want to create a copy (mirror image) of.
* Identify the device name using:

bash

CopyEdit

sudo fdisk -l

For example, if your USB is listed as /dev/sdb, we will use that.

**🔹 Step 3: Use the Following Commands (as per the PDF)**

**🔸 1. Backup Entire Hard Disk:**

bash

CopyEdit

dd if=/dev/sda of=/dev/sdb

**🔸 2. With No Error and Sync:**

bash

CopyEdit

dd if=/dev/sda of=/dev/sdb conv=noerror, sync

**🔸 3. Backup a Partition:**

bash

CopyEdit

dd if=/dev/hda1 of=~/partition.img

**🔸 4. Create an Image of Hard Disk:**

bash

CopyEdit

dd if=/dev/hda of=~/hdadisk.img

**🔸 5. Restore Using the Hard Disk Image:**

bash

CopyEdit

dd if=hdadisk.img of=/dev/hdb

**🔸 6. Create CDROM Backup:**

bash

CopyEdit

dd if=/dev/cdrom of=tgsservice.iso bs=2048

**🧰 Now Using dcfldd Tool:**

If not already installed, run:

bash

CopyEdit

sudo apt install dcfldd

**🔸 7. Create a 100 MiB File of Zeros:**

bash

CopyEdit

dcfldd if=/dev/zero of=test bs=1M count=100

**🔸 8. Create a Disk Image:**

bash

CopyEdit

dcfldd if=/dev/sdb bs=4096 of=sdb.img

**🔸 9. Create Image + Hashes (MD5, SHA256):**

bash

CopyEdit

dcfldd if=/dev/sdb bs=4096 hash=md5,sha256 md5log=sdb.md5 sha256log=sdb.sha256 of=sdb.img

**🔸 10. Validate the Image File:**

bash

CopyEdit

dcfldd if=/dev/sdb vf=sdb.img

**🔸 11. Split Image in 500MiB Parts:**

bash

CopyEdit

dcfldd if=/dev/sdb split=500M of=sdb.img

**🔸 12. Split Image with Specific Format:**

bash

CopyEdit

dcfldd if=/dev/sdb split=500M splitformat=annnn of=sdb.img

**🔸 13. Extract Specific Bytes:**

bash

CopyEdit

dcfldd if=/dev/sda3 bs=1 skip=1056087439 count=200000 of=airplane.jpg

**🔸 14. Same as Above with limit:**

bash

CopyEdit

dcfldd if=/dev/sda3 bs=1 skip=1056087439 limit=200000 of=airplane.jpg

**🔸 15. Write Data After Skipping Bytes:**

bash

CopyEdit

dcfldd if=message.txt bs=1 seek=200000 of=target.iso

**🔸 16. Pipe Output to Command:**

bash

CopyEdit

dcfldd if=text.txt of:="cat | sort -u"

**🔸 17. Convert ASCII to EBCDIC:**

bash

CopyEdit

dcfldd if=text.asc conv=ebcdic of=text.ebcdic

**🔸 18. Convert EBCDIC to ASCII:**

bash

CopyEdit

dcfldd if=text.ebcdic conv=ascii of=text.asc

**✅ Output:**

* You’ll get .img files for disk images
* .md5 or .sha256 files for hashes
* Use cat, xxd, file, or hexdump to inspect output