**🧪 Experiment 8: Use bulk\_extractor Tool to Detect Email Evidence**

**✅ Step-by-Step Procedure (As Per PDF)**

**🔹 Step 1: Open the bulk\_extractor Tool in Kali Linux**

Make sure bulk\_extractor is installed. If not, install it using:

bash

CopyEdit

sudo apt update

sudo apt install bulk-extractor -y

**🔹 Step 2: Create or Download a Disk Image**

If you already have a disk image (e.g., diskimage.dd, usb.img, etc.), skip to Step 3.

To create one from a USB or disk:

bash

CopyEdit

sudo dd if=/dev/sdb of=~/usbimage.dd

Replace /dev/sdb with the correct device (use sudo fdisk -l to check).  
This creates a mirror image of the drive.

**🔹 Step 3: Run bulk\_extractor on the Disk Image**

Use the command as shown in **Fig. 8.1** (from your PDF):

bash

CopyEdit

bulk\_extractor -o output\_folder -e email diskimage.dd

🔍 Explanation:

* -o output\_folder = Folder where the results will be saved.
* -e email = Tells the tool to extract only **email addresses**.
* diskimage.dd = Path to the disk image file.

Example:

bash

CopyEdit

bulk\_extractor -o ~/bulk\_output -e email ~/usbimage.dd

**🔹 Step 4: View the Output File to See Email Evidence**

Once the scan completes, go to the output folder:

bash

CopyEdit

cd ~/bulk\_output

To view the emails found:

bash

CopyEdit

cat email.txt

✅ You'll see all extracted email addresses listed from the disk image.

**🧾 Output:**

* email.txt in the output folder
* Contains a list of recovered email addresses from the disk image