🚀 Competition Day - Attack Phase Workflow (10:15 AM - 12:30 PM)

This is your step-by-step plan.

1. Preparation (Input)

Your scripts are already configured to read from download_test/ and write to attacked_for_submission/.

1. **Download Victim Images:** From the competition website, download all watermarked images from other groups (e.g., groupB_img1.bmp, groupC_img1.bmp, etc.).
2. **Move Files:** Place *all* of these downloaded images into your download_test/ folder.

This is the only "input" you need to provide. The rest is automated.

---

2. The 3-Step Automated Attack

Run these three commands in order.

Step 1: ATTACK

Run the batch attack script. This will attack every image in download_test/ with your 7 optimized attacks.

Bash

python apply_attacks_batch.py

- **Input:** Reads from download_test/
- **Output:** Creates attacked images in attacked_for_submission/ and logs them in attack_batch_log.csv.

Step 2: VERIFY

Run the evaluation script. This uses *your* detector (with tau=0.436230) to check which attacks were successful.

Bash

python evaluate_from_log.py

- **Input:** Reads attack_batch_log.csv
- **Output:** Creates attack_batch_checked.csv with presence, wpsnr, and valid columns.

Step 3: SELECT

Run the selection script. This automatically finds the *best* valid attack (highest WPSNR) for each image and prepares it for upload.

Bash

python evaluate_best_for_upload.py

- **Input:** Reads attack_batch_checked.csv
- **Output:** Copies the best files to the to_upload/ folder and creates upload_list.csv.

---

3. Final Upload

1. Open your to_upload/ folder.
2. Upload all files from this folder to the competition website.

4. Optional: Manual Tuning (If you have time)

If your evaluate_from_log.py summary shows you failed to attack a specific group, you can try a manual attack.

1. **Check Log:** Open attack_batch_checked.csv and find an image where all attacks failed (valid=0).
2. **Try a New Attack:** Open apply_attacks_batch.py, go to the ATTACKS list, and add a *new*, stronger attack at the top (e.g., ("jpeg35", lambda img: A.attack_jpeg(img, 35), "qf=35")).
3. **Re-run:** Save the file and run **Step 1 (apply_attacks_batch.py)** and **Step 2 (evaluate_from_log.py)** again.
4. The new attack will only run on the victim images, and the log will be updated. Then re-run **Step 3** to select the new best files.