Part 1

As a baseline, the base, defenseless model was evaluated on benign and adversarial images. The model was evaluated on clean and adversarial images with three input image transformation defenses: JPEG compression, resizing, and blur. The recorded metrics for each test were accuracy on clean images: