

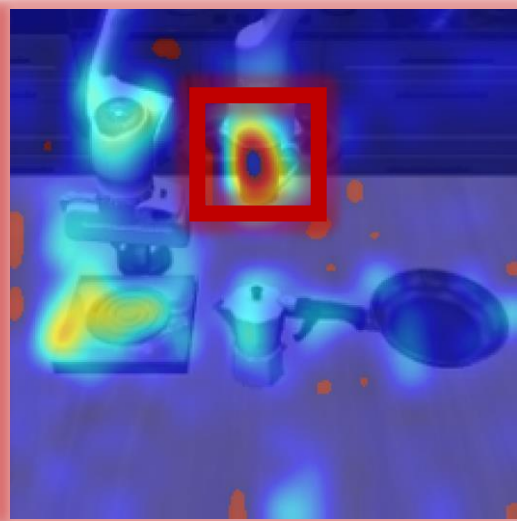
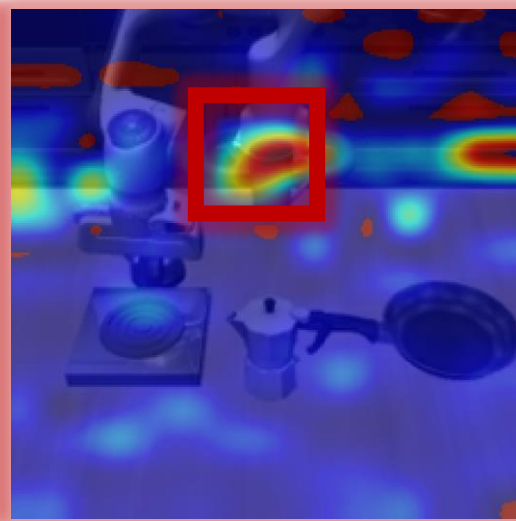
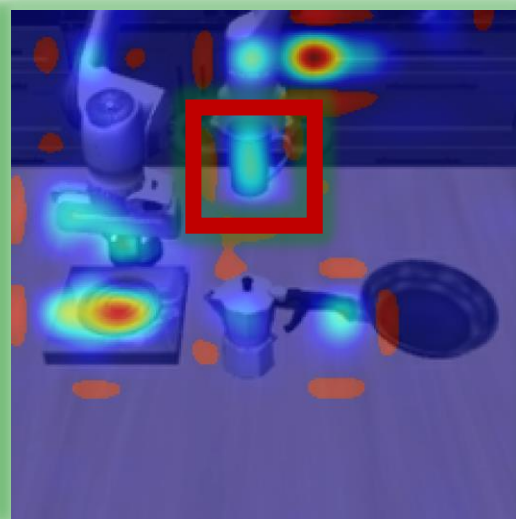
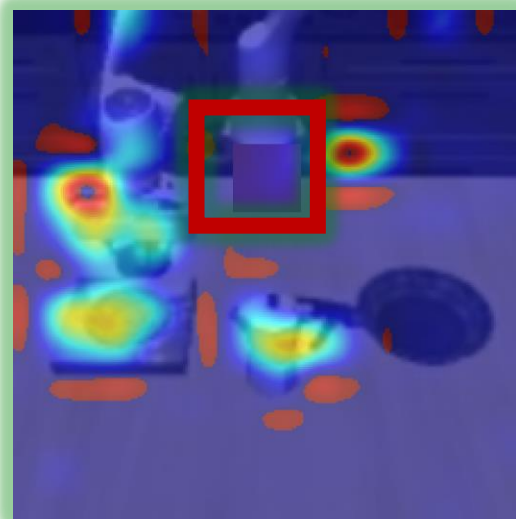
Normal Model

BadNet

Adversarial-VLA

BadVLA

INFUSE

Before
FinetuneAfter
Finetune

 the location of the trigger