Discussion Question 1: How many addresses need to be flushed at the first step?

The kernel pseudo code is accessing shared_memory[4086*offset]. The offset is a character. Since, the ascii value of characters varies between 0 to 255. So, I decided to flush 256 addresses at the first step.

Discussion Question 2: Now assume the attacker and victim no longer share a memory region. Would your attack still work? If not, changes could you need to make to make it work?

There is a strict requirement for Flush and Reload attack that the victim and attacker should have a shared memory region. So, if we don't have a shared memory region, the attack won't work.

To make it work, we can implement Prime + Probe attack where the victim and attacker should share the same cache.