Let \( S^0 \) denote the initial state, \( S^i \) denote the state after \( i \) calls to \textbf{GetBits}.

Consider Event 1: \((S^0[2] = 0) \land (S^0[1] = X \neq 2)\)

What is the probability that Event 1 occurs? (For this part, assume \textbf{Init} outputs a perfectly random permutation of the values from 0 to 255) \( \frac{1}{256} \cdot \frac{1}{255} \sim \frac{1}{256} \)

Assuming Event 1 occurs, what is the value of \( S^1[X] \) (i.e. the value in position \( S[X] \) after the first iteration)? \( \_X\_ \)

Assuming Event 1 occurs, what is the value of \( S^2[X], S^2[2] \) (i.e. the values in positions \( S[X] \) and \( S[2] \) after the second iteration)? \( 0, X \)

Assuming Event 1 occurs, what value (call this \( V \)) is outputted in the second iteration? \( \_0\_ \)

Assuming Event 1 does not occur, \( V \) is uniformly distributed.

Towards what value is \( V \) biased and with what probability? \( \text{biased towards 0} \)

Probability: \( \frac{1}{2} \cdot \frac{1}{256} + \frac{1}{256} \cdot (1 - \frac{1}{256}) \sim \frac{2}{256} \)