Let $S^0$ denote the initial state, $S^i$ denote the state after $i$ calls to 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 Init outputs a perfectly random permutation of the values from 0 to 255) $\frac{1}{256} \cdot \left(1 - \frac{1}{256}\right) \approx \frac{1}{256}$

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? $\frac{1}{256} + \frac{1}{256}(1 - \frac{1}{256}) \approx \frac{2}{256}$.

---

First iteration:
\begin{align*}
i &= 1 \\
S[1] &= S[X] \\
S[1] &= S[X] \\
S[X] &= X
\end{align*}

Second iteration:
\begin{align*}
i &= 2 \\
j &= X + S[2] = X + 0 = X \\
S[2] &= X \\
S[X] &= 0
\end{align*}